TASK ORDER:

GST0012AJ0077

Cyber Forensics Support

in support of:

Defense Cyber Crime Center (DC3)

issued to:

Lockheed Martin Integrated Systems Inc.

Alliant
Contract: GS00Q09BGD0039

issued by:
The Federal Systems Integration and Management Center (FEDSIM)
1800 F St NW
Suite 3100
Washington DC VA 20405

FEDSIM Project Number 26218DEM

NOTE: The section numbers in this Task Order (TO) correspond to the section numbers in the Alliant Contract. Section B of the contractor's Alliant Contract is applicable to this TO and is hereby incorporated by reference. In addition, the following applies:

B.1 GENERAL

The work shall be performed in accordance with all sections of this TO and the contractor's Basic Contract, under which the resulting TO will be placed.

B.5 CONTRACT ACCESS FEE

The General Services Administration's (GSA) operating costs associated with the management and administration of this contract are recovered through a Contract Access Fee (CAF). The amount of the CAF is ¾ % (i.e., (.0075)) of the total price/cost of contractor performance. Each TO issued under this contract shall have a separate Contract Line Item Number (CLIN) to cover this access fee, and this CAF shall be obligated at TO award. The following access fee applies to the TO issued under this contract.

GSA-Issued Task Orders:
Orders in excess of $13.3 million/year are capped at $100,000 per year.

B.6 ORDER TYPES

The contractor shall perform the effort required by this task order on a Firm Fixed Price (FFP) basis for CLINs 0001, 1001, 2001, 3001, 4001, and 0002, 1002, 2002, 3002, 4002, Cost Plus Fixed Fee (CPFF) for CLINs 0003 1003, 2003, 3003, 4003 and Not to Exceed (NTE) basis for CLINs 0004, 1004, 2004, 3004, 4004, 0005, 1005, 2005, 3005, 4005, 0006, 1006, 2006, 3006, 4006, and 0007, 1007, 2007, 3007, 4007.

B.7 ORDER PRICING (ALL ORDER TYPES)

The following abbreviations are used in this price schedule:

CPFF	Cost-Plus-Fixed-Fee
CLIN	Contract Line Item Number
FFP	Firm-Fixed-Price
ODC	Other Direct Cost
NTE	Not-to-Exceed

B.7.1.1 BASE PERIOD:

CLIN	Description	QTY	Unit	Total Firm Fixed Price
0001	Program Management Support (Task 1)	(b) (4)		
0002	Help Desk Support (Task 2)			

LABOR CLIN CPFF TERM

CLIN	Description	Level of Effort/ # of Hours	Estimated Cost	Fixed Fee	Total Estimated Cost Plus Fixed Fee
0003	Cyber Forensics Support (Task Areas 3, 4, 5, 6, and 7)	407228	(b) (4)		
0003B	Optional Surge Support (Task Area 8)	159,362			

TRAVEL, TOOLS and ODCs CLINs

CLIN	Description		Total Ceiling Price
0004	Long Distance Travel Including Indirect Handling Rate (b) (4)	NTE	(b) (4)
0005	Tools Including Indirect Handling Rate (b) (4)	NTE	
0006	ODCs Including Indirect Handling Rate (b) (4)	NTE	
0007	Contract Access Fee	NTE	

GRAND TOTAL BASE PERIOD CLINS: $73,775,207

B.7.1.2 OPTIONAL PERIOD 1:

CLIN	Description	QTY	Unit	Total Firm Fixed Price
1001	Program Management Support (Task Area 1)	(b) (4)		
1002	Help Desk Support (Task Area 2)			

LABOR CLIN CPFF TERM

CLIN	Description	Level of Effort/# of Hours	Estimated Cost	Fixed Fee	Total Estimated Cost Plus Fixed Fee
1003	Cyber Forensics Support (Task Areas 3, 4, 5, 6, and 7)	(b) (4)			
1003B	Optional Surge Support (Task Area 8)				

TRAVEL, TOOLS and ODCs CLINs

CLIN	Description		Total Ceiling Price
1004	Long Distance Travel Including Indirect Handling Rate (b) (4)	NTE	(b) (4)
1005	Tools Including Indirect Handling Rate (b) (4)	NTE	
1006	ODCs Including Indirect Handling Rate (b) (4)	NTE	
1007	Contract Access Fee	NTE	

GRAND TOTAL OPTIONAL PERIOD 1 CLINS: $83,551,780

B.7.1.3 OPTIONAL PERIOD 2:

CLIN	Description	QTY	Unit	Total Firm Fixed Price
2001	Program Management Support (Task Area 1)	(b) (4)		
2002	Help Desk Support (Task Area 2)			

LABOR CLIN CPFF TERM

CLIN	Description	Level of Effort/ # of Hours	Estimated Cost	Fixed Fee	Total Estimated Cost Plus Fixed Fee
2003	Cyber Forensics Support (Task Areas 3, 4, 5, 6, and 7)	(b) (4)			
2003B	Optional Surge Support (Task Area 8)				

TRAVEL, TOOLS and ODCs CLINs

CLIN	Description		Total Ceiling Price
2004	Travel Including Indirect Handling Rate (b) (4)	NTE	(b) (4)
2005	Tools Including Indirect Handling Rate (b) (4)	NTE	
2006	ODCs Including Indirect Handling Rate (b) (4)	NTE	
2007	Contract Access Fee	NTE	

GRAND TOTAL OPTIONAL PERIOD 2 CLINS: $91,279,706

B.7.1.4 OPTIONAL PERIOD 3:

CLIN	Description	QTY	Unit	Total Firm Fixed Price
3001	Program Management Support (Task Area 1)	(b) (4)		
3002	Help Desk Support (Task Area 2)			

LABOR CLIN CPFF TERM

CLIN	Description	Level of Effort/ # of Hours	Estimated Cost	Fixed Fee	Total Estimated Cost Plus Fixed Fee
3003	Cyber Forensics Support (Task Areas 3, 4, 5, 6, and 7)	(b) (4)			
3003B	Optional Surge Support (Task Area 8)				

TRAVEL, TOOLS and ODCs

CLIN	Description		Total Ceiling Price
3004	Travel Including Indirect Handling Rate (b) (4)	NTE	(b) (4)
3005	Tools Including Indirect Handling Rate (b) (4)	NTE	
3006	ODCs Including Indirect Handling Rate (b) (4)	NTE	
3007	Contract Access Fee	NTE	

GRAND TOTAL OPTIONAL PERIOD 3 CLINS: $100,536,661

B.7.1.5 OPTIONAL PERIOD 4:

CLIN	Description	QTY	Unit	Total Firm Fixed Price
4001	Program Management Support (Task Area 1)	(b) (4)		
4002	Help Desk Support (Task Area 2)			

LABOR CLIN CPFF TERM

CLIN	Description	Level of Effort/ # of Hours	Estimated Cost	Fixed Fee	Total Estimated Cost Plus Fixed Fee
4003	Cyber Forensics Support (Task Areas 3, 4, 5, 6, and 7)	(b) (4)			
4003B	Optional Surge Support (Task Area 8)				

TRAVEL, TOOLS and ODCs CLINs

CLIN	Description		Total Ceiling Price
4004	Travel Including Indirect Handling Rate (b) (4)	NTE	(b) (4)
4005	Tools Including Indirect Handling Rate (b) (4)	NTE	
4006	ODCs Including Indirect Handling Rate (b) (4)	NTE	
4007	Contract Access Fee	NTE	

GRAND TOTAL OPTIONAL PERIOD 4 CLINS: $105,348,222

GRAND TOTAL ALL CLINS: $454,491,576

B.12 SECTION B TABLES

B.12.1 INDIRECT/MATERIAL HANDLING RATE

Travel, Tools, and ODC costs incurred may be burdened with the Contractor's indirect/material handling rate in accordance with the Contractor's disclosed practices and if such indirect/material handling rate is not included in the fully burdened labor rate. If no indirect/material handling rate is allowable in accordance with the Contractor's disclosed practices, no indirect/material handling rate shall be applied to or reimbursed on such costs. If no rate is specified in the basic contract, none shall be applied in this TO.

B.13 INCREMENTAL FUNDING

B.13.1 INCREMENTAL FUNDING LIMITATION OF GOVERNMENT'S OBLIGATION

Incremental funding for CLINs 0001 through 2001, 2002, 2003, 2004, 2005 and 2007 is currently allotted and available for payment by the Government. Additional incremental funding for these CLINs will be allotted and available for payment by the Government as the funds become available. The estimated period of performance covered by the allotments for the mandatory CLINs is from award through April 15, 2015 unless otherwise noted in Section B.7.1.1. This Task Order will be modified to add funds incrementally up to the maximum of $454,491,575 over the period of performance of this TO. These allotments constitute the estimated cost for the purpose of Federal Acquisition Regulation (FAR) Clause 52.232-22, Limitation of Funds, which applies to this TO on a CLIN-by-CLIN basis.

Incremental Funding Chart

CLIN	ESTIMATED COST/PRICE	FIXED FEE	Total	FUNDED COST	FUNDED FEE	Total
0001						
0002						
0003						
0003B						
0004						
0005						
0006						
0007						
Total						
1001						
1002						
1003						
1003B						
1004						
1005						
1006						
1007						
Total						
2001						
2002						
2003						
2003B						
2004						
2005						
2006						
2007						
Total						
3001						
3002						
3003						
3003B						
3004						
3005						
3006						
3007						
Total						
4001						
4002						
4003						
4003B						
4004						
4005						
4006						
4007						
Total						
GRAND TO	(b) (4)		$454,491,576	(b) (4)	(b) (4)	$145,133,497.88

(b) (4)

B.14 REPRICING (Applies to CLINS X003, X003b, X004, X005, and X006 only)

Once the Forward Pricing Rate Proposals that Lockheed Martin and its segments have submitted to the cognizant Defense Contract Management Offices (DCMA) and the Defense Contract Audit Agency's (DCAA) have been reviewed/audited and an Forward Pricing Rate Agreement has been issued by DCMA a downward adjustment may result. In addition, a downward adjustment may result once the cost impact of the organizational changes of the Lockheed Martin Information Systems and Global Solutions Development and Engineering Services Segments have been reviewed and audited by the cognizant Defense Contract Management Offices (DCMA) and the Defense Contract Audit Agency's (DCAA).

C.1 BACKGROUND

The Department of Defense (DoD) relies heavily on computer systems to meet its mission and to conduct daily operations. Due to the vital role computer systems play in the operation of the military, computer intrusion and other computer related crimes have the potential to drastically affect the U.S. military. The Department of Defense Cyber Crime Center (DC3) was established in October 2002, as a Department of Defense (DoD) center of excellence to efficiently organize, equip, train, and employ resources to more effectively address the proliferation of computer crimes affecting the DoD. Its mission is to deliver superior digital and multimedia (D/MM) forensics and multimedia lab services, cyber technical training, research, development, testing and evaluation capabilities supporting cyber counterintelligence and counterterrorism, criminal investigations, intrusion forensics, and information operations for the Department of Defense. This includes processing digital evidence and analysis of electronic media in support of criminal law enforcement and DoD counterintelligence investigations and activities, providing D/MM forensic examinations and training to DoD members to ensure information systems are secure from unauthorized use, and performing research, development, testing, and evaluation (RDT&E) of D/MM forensic techniques to remain on the leading edge of future investigations.

The Secretary of the Air Force (AF) serves as the DoD Executive Agent for these activities and the Commander of the Air Force Office of Special Investigations (AFOSI) provides overall program management.

The DC3 is composed of five (5) directorates, the Defense Computer Forensics Laboratory (DCFL), the Defense Cyber Crime Institute (DCCI), and the Defense Cyber Investigations Training Academy (DCITA), the DoD-Defense Industrial Base Collaborative Information Sharing Environment (DCISE), and the Defense Cyber Crime Center-Analytical Group (DC3-AG). Located in Anne Arundel County Maryland, DC3 serves the DoD and other U.S. Federal agencies throughout the world. The DC3 organization consists of a mix of Government, civilian, and contractor support personnel. The DC3 environment is dynamic and constantly evolving which contributes to priorities frequently changing. As the mission of DC3 continues to expand and advance, the requirement for information technology support will continue to grow.

C.2 PURPOSE

The task order will provide mission critical digital and multimedia (D/MM) forensic information technology (IT) technical and managerial examination, research, and development support services, and cyber analytical services to the Defense Cyber Crime Center (DC3).

C.3 DC3 Mission

DC3 is operationally aligned into the organizations described below each with interrelated missions and support requirements.

C.3.1 Defense Computer Forensics Laboratory (DCFL)

D/MM forensics is science applied to computers through the use of analytical and investigative techniques to identify, collect, examine and preserve evidence/information which is magnetically stored or encoded. The DCFL mission provides digital evidence processing and analysis for DoD, sets DoD guidelines for D/MM forensics analysis, fosters forensic media analysis and RDT&E projects, and conducts liaison by partnering with Governmental and private industry computer security officials to keep abreast of cutting edge technology. This includes criminal, counterintelligence, counterterrorism, and fraud investigations of defense criminal investigative organizations (DCIO's) and DoD counterintelligence activities, as well as safety investigations, Inspector General directed inquiries and commander inquires. DCFL specifically functions in the following ways:

- Forensic analysis of electronic media
- Assists in on-site electronic media examination and analysis in support of investigative and operational requirements
- Consults on electronic media related investigations and activities
- Provides expert testimony in court proceedings
- Consults on D/MM forensics
- Serves as DoD authority on D/MM forensic matters DCFL offers DoD the ability to process digital and analog evidence in an attempt to prosecute individuals using computer systems or digital data to aid in criminal activity.

DCFL received accreditation under the American Society of Crime Laboratory Directors (ASCLD) laboratory accreditation program in September 2005 and is currently the world's largest fully accredited D/MM forensics lab.

C.3.2 Defense Cyber Crime Institute (DCCI)

The Defense Cyber Crime Institute (DCCI) develops the foundation D/MM forensics standards based on science and law. DCCI serves as a resource for research to produce tools and procedures to include providing legally and scientifically accepted standards, techniques, methodologies, tools and technologies on D/MM forensics and related technologies. DCCI strives to meet the current and future needs of DoD counterintelligence, intelligence, information assurance, information operations and law enforcement communities. This is accomplished by:

- Research and Development
- Test and Evaluation

One of the critical missions of DCCI is to provide support to DCFL as an accredited forensics lab. The essential criteria for a digital crime lab is to have all of their tools, both hardware and software, tested and validated that they are forensically sound. DCCI supports this effort by performing these tests and validations.

C.3.3 Defense Cyber Investigations Training Academy (DCITA)

The Defense Cyber Investigations Training Academy (DCITA) develops and delivers computer investigation training (CIT) courses for DoD organizations, defense criminal investigative

organizations, military counterintelligence agencies, and law enforcement organizations. The purpose of the training is to ensure defense information systems are secure from unauthorized use, counterintelligence, and criminal and fraudulent activities. DCITA training includes:

- Computer search and seizure techniques
- Network intrusions investigations
- Forensic computer media analysis
- Basic and advanced forensic examinations
- Online undercover techniques

Support to DCITA is not a requirement of this Task Order (except for subtasks 3.14.1 and 3.15).

C.3.4 DoD-Defense Industrial Base Collaborative Information Sharing Environment (DCISE)

The mission of the DCISE is to secure critical DoD programs and technology by protecting DoD Controlled Unclassified Information (CUI) resident on Defense Industrial Base (DIB) networks, through collaboration with industry.

In addition to threat information sharing, DoD is beginning collaboration efforts with DIB partners on technology solutions such as; encrypted data at rest or in transit, host-based security systems, and thin-client solutions for internal DIB intelligence dissemination. These are just some of the methods being considered to help protect sensitive hosted and transitory data.

In coordination with DHS, the DoD-DIB model for information sharing will be extended to other critical Infra Sectors (financial, chemical, IT, telecommunication). DCFL/DCISE intends to share successful methods of detection and protection with the DHS to extend its use with their industrial partners.

C.3.5 Support to Defense Cyber Crime Center Analytical Group (DC3-AG)

DC3 is required to work in concert with the National Cyber Investigative Joint Task Force, DC3-AG and other United States Government (USG) Cyber Centers to protect information stored on DIB networks as well as USG networks. The DCISE directly collaborates with the DC3 Analytical Group (AG) staff to support this type of action.

C.3.6 Support to Network Management Organization (NMO)

The Network Management Office (NMO) was created in 1998 and currently provides information technology (IT) and telecommunications support. These critical systems require 24 hours a day operational availability seven (7) days a week (see Section F.4 for "on-call" support requirements). NMO is currently responsible for over 12 separate network and telecommunications systems of all classification levels serving more than 315 customers throughout the DC3 organization. The NMO also maintains and supports all Corporate and Forensics applications that run on forensically sound workstations, several of which are mission critical.

C.3.7 Deleted

C.4 CURRENT IT/NETWORK ENVIRONMENT

DC3 relies extensively on information systems to support operations and to store sensitive information. DC3 critical systems require 24 hours a day operational availability seven (7) days a week. All IT operations must be in accordance with all DoD operational security implementation guidelines, DoD directives, and Defense Information Systems Agency (DISA), DoD and AF instructions and be in adherence with DoD Directive 8570.1**.**

DC3 operates and maintains (1) Non-classified Internet Protocol (IP) Routing Network (NIPRNET), one (1) Secret Internet Protocol Routing Network (SIPRNET) network, (1) Joint Worldwide Intelligence Communications System (JWICS) and multiple stand-alone forensic/examination networks that provide processing and communications support.

The NIPRNET provides seamless interoperability for unclassified combat support applications, as well as controlled access to the Internet. SIPRNET is a Secret IP Router Network and is DoD's largest interoperable command and control data network, supporting the Global Command and Control System (GCCS), the Defense Message System (DMS), collective planning and numerous other classified warfighter applications.

Other operating systems include all versions of Microsoft Windows, Linux, and Sun Solaris.

Other applications include network-messaging, E-mail (Electronic Mail), Internet access, Footprints Help Desk, a Digital Forensics Information (DFI) Portal, StarLims Laboratory Management System.

C.5 SCOPE AND OBJECTIVES

C.5.1 SCOPE

The scope of this effort is to provide technical, functional, and managerial information technology (IT) support to the DC3(and related organizations) by providing D/MM forensic examination, analysis, research, development, test and evaluation initiatives, network and telecommunications support, information protection and information assurance, quality assurance, and D/MM forensic operational support.

The contractor shall be required to travel to CONUS and OCONUS sites to provide evidence examination and to provide testimony in court proceedings.

C.5.2 OBJECTIVES

The Department of Defense (DoD) relies heavily on computer systems to meet its mission and to conduct daily operations. Due to the vital role computer systems play in the operation of the military, computer intrusion and other computer related crimes have the potential to drastically affect the U.S. military. The Task Order requirements are highly specialized and the support needed sets standards for digital evidence processing, analysis, and diagnostics for any DoD or other USG investigation that requires computer forensic support to detect, enhance, or recover digital media, including audio and video. DC3 assists in criminal, counterintelligence, counter terrorism, and fraud investigations of the Defense Criminal Investigative Organizations (DCIOs) and DoD counterintelligence activities. Contractor support will be required to testify in court on chain of custody and forensics methodology and standards used.

DC3 requires proven technical experience and expertise in managing a cyber crime lab facility (DCFL) that provides comprehensive evidentiary analysis of material. DCFL has organized digital forensic examinations within an industrial process that is unmatched elsewhere in terms of its scope. It is accredited by the American Society of Crime Lab Directors, Laboratory Accreditation Board (ASCLD/LAB), the preeminent authority for accredited crime labs in the United States. Maintaining this accreditation is critical to the future success of the DCFL. The lab's prime focus is on intrusions, national security cases and Special Access Program support.

The objectives of this task order are to provide mission critical digital forensic information technology (IT) technical and managerial examination, research, cyber analysis, and development support services to the Defense Cyber Crime Center (DC3).

C.6 TASKS

C.6.1 TASK AREA 1--PROVIDE DC3 PROGRAM MANAGEMENT (CLIN 0001)

The contractor shall provide on-site program management support under this Task Order. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the requirements identified in this Statement of Work (SOW). The contractor shall identify a Program Manager (PM) by name, who shall provide management, direction, administration, quality assurance, and leadership of the execution of this task order. The PM shall serve as the primary interface and point of contact with the Government program authorities and representatives on technical program/project issues.

The contractor shall facilitate Government and contractor communications and all activities necessary to ensure the accomplishment of timely and effective support, performed in accordance with the requirements contained in this task order (TO). The contractor shall provide all necessary personnel, administrative, financial, paralegal, and managerial resources necessary for the support of this TO.

The contractor shall use proven methodologies that assure that all task order activities are identified, documented, and tracked so that the task order will continuously be evaluated and

monitored for timely and quality service. The contractor shall notify the FEDSIM Contracting Officer's Representative (COR) and DC3 Technical POC (TPOC) of any technical, financial, personnel, or general managerial problems encountered throughout the task order period of performance.

C.6.1.1 SUBTASK 1.1 -- COORDINATE A PROJECT KICKOFF MEETING

The contractor shall schedule and coordinate a Project Kick-Off Meeting at the location approved by the Government. The meeting will provide an introduction between the contractor personnel and Government personnel who will be involved with the task order. The meeting will provide the opportunity to discuss technical, management, and security issues, and travel authorization and reporting procedures. At a minimum, the attendees shall include key contractor personnel, representatives from the directorates, other key Government personnel, and the Federal Systems Integration and Management Center (FEDSIM) Contracting Officer's Representative (COR). The contractor shall provide a Kick-off agenda that will include, but not limited to, the following **[Section F, Deliverable 01]**

- Introduction of personnel
- Overview of project tasks
- Travel notification and processes
- Transition Plan
- Discussion on PMP
- Security requirements/issues/facility access procedures
- Invoice procedures
- Work Schedules
- Leave notification and processes
- Points of contact
- Other logistics issues
- Contract Notification
- Final Quality Control Plan
- Additional issue of concern
- Forensic Examination Training Requirements
- Cyber Analyst Training Requirements

The contractor shall provide a draft copy of the agenda for review and approval by the FEDSIM COR and DC3 TPOC prior to finalizing. The Government will provide the contractor with the number of participants for the kick-off meeting and the contractor shall provide sufficient copies of the presentation for all present **[Section F, Deliverable 02].**

C.6.1.2 SUBTASK 1.2 -- PREPARE A PROGRAM MANAGEMENT PLAN (PMP)

The Contractor shall document all support requirements in a PMP. The PMP shall describe the management approach. The PMP shall detail Standard Operating Procedures (SOPs) for all tasks. The PMP shall include milestones, tasks, and subtasks required in this task order. The PMP shall provide for an overall Work Breakdown Structure (WBS) and associated responsibilities and

partnerships between Government organizations. The PMP shall include the contractor's Quality Control Plan (QCP).

The Contractor shall provide the Government with a draft PMP **[Section F, Deliverable 03]** for presentation at the Kick Off meeting, of which the Government will make comment. Following the Kick Off meeting, the contractor shall revise the PMP to incorporate Government comments **[Section F, Deliverable 04].** The PMP shall contain, at a minimum, the following per task:

- Task Methodologies
- Staffing Plan Per Task
- Deliverables Per Task
- Quality Control Procedures
- Points of Contact
- General Operating Procedures for
  - Travel
  - Work Hours
  - Leave
  - Deliverables
  - Problem/Issue Resolution Procedures
- Program/Performance Metrics
- Government and Contractor approved guidelines for deliverable deadlines.

The PMP shall contain a separate schedule for each organizational area that contains deliverable milestones and deadlines. Deliverables with short suspense's will be excluded from the PMP.

The PMP shall include, as attachments, individual Project Plans for long term development projects, e.g., Lab Modernization Plan, Maintenance of DFI Portal, network consolidation/virtualization plan, and Special Studies Plan.

As part of the PMP, the contractor shall develop a draft and final Work Breakdown Structure (WBS) that delineates the relationship of Section C Tasks, the contractors identified task activities and work packages, and estimated resources required to successfully executive this TO. Subsequent revisions to the WBS must be submitted to the Government for approval. The contractor shall maintain the WBS to reflect current progress throughout the life of the project.

C.6.1.2.1 UPDATE THE PROJECT MANAGEMENT PLAN (PMP)

The PMP is an evolutionary document. It shall be updated quarterly. The contractor shall work from a Government approved PMP. The contractor shall work from a new version of the PMP once approved by the Government **[Section F, Deliverable 05**].

C.6.1.3 SUBTASK 1.3 -- Prepare Management Reports

Monthly Status Report (MSR)

The contractor Program Manager shall develop and provide a MSR by the 10th of each month via electronic mail to the TPOC and the COR **[Section F, Deliverable 06].**

The MSR shall include the following:

- Activities during reporting period, by task (Include: On-going activities, new activities, activities completed; progress to date on all above mentioned activities). Start each section with a brief description of the task.
- Problems and corrective actions taken. Also include issues or concerns and proposed resolutions to address them.
- Personnel gains, losses and status (security clearance, training, etc.).
- Government actions required.
- Schedule (Shows major tasks, milestones, and deliverables; planned and actual start and completion dates for each).
- Performance during the reporting period for each performance measure defined in the Quality Control Plan.
- Summary of trips taken, conferences attended, etc. (Attach trip reports to the MSR for reporting period).
- Accumulated invoiced cost for each CLIN up to the previous month.
- Projected cost of each CLIN for the current month.
- Comparison data / monthly performance reports.

The contractor shall reconcile the MSR with each invoice such that they can be matched month by month. The monthly status report shall be prepared in accordance with the sample in **Section J, Attachment A**.

TRIP REPORTS

The Government will identify the need for a Trip Report **[Section F, Deliverable 07]** when the request for travel is submitted. The Trip report shall include the following information:

- Personnel traveled
- Dates of travel
- Destination(s)
- Purpose of trip
- Cost of the trip
- Approval Authority
- Summary of events

The contractor shall reconcile the Trip Reports with each invoice such that they can be matched month by month. The Contractor shall keep a summary of all long-distance travel.

MEETING REPORTS

The contractor shall submit Meeting Reports to document results of meetings within 72 hours. **[Section F, Deliverable 08].** The Meeting Report shall include the following information:

- Meeting attendees
- Meeting dates
- Meeting location
- Purpose of meeting
- Summary of events

The contractor shall reconcile their Meeting Report with official meeting minutes if published and advise the Government lead accordingly.

PROBLEM NOTIFICATION REPORTS (PNRs)

The contractor shall file a Problem Notification Report (PNR) **[Section F, Deliverable 09]** to notify the COR of TO issues such as potential cost/schedule overruns/impacts, assumptions upon which tasks were based that have changed or were incorrect, etc. The PNR shall be prepared in accordance with the sample in **Section J, Attachment J**.

WEEKLY E-MAIL STATUS REPORTS

The contractor shall provide weekly e-mail status reports to Government Task Managers providing the status, adherence to the project plan, timelines, and notification of any problems. The report shall be submitted in Word and/or Excel format via email to the corresponding Government stakeholders **[Section F, Deliverable 10]**.

C.6.1.4 SUBTASK 1.4 -- CONVENE TECHNICAL STATUS MEETINGS

The Program Manager (PM) shall convene a monthly contract activity and status meeting with the TPOC, COR, and other key Government stakeholders. The purpose of this meeting is to ensure all stakeholders are informed of the monthly activity and status report, provide opportunities to identify other activities and establish priorities, and coordinate resolution of identified problems or opportunities. The Program Manager shall provide minutes of these meetings, including attendance, issues discussed, decisions made, and action items assigned, to the COR within five (5) calendar days following the meeting **[Section F, Deliverable 11].**

C.6.1.5 SUBTASK 1.5 -- DC3 ORGANIZATIONAL MANAGEMENT SUPPORT

In addition to managing the other tasks within the statement of work the contractor shall provide direct support to DC3's overall functionality, operability and sustainment as a National Cyber Center.

C.6.1.5.1 FUNCTIONAL MANAGEMENT

The contractor shall respond to inquiries, obtain, route, and relay information, coordinate and update schedules, coordinate site visits and tours, maintain logs, coordinate and support meetings

and internal functions, assist with travel and security documentation and serve as the DC3 main point of initial contact.

The contractor shall maintain and administer all DC3 official documents and templates. The contractor shall develop, maintain, and manage file plans. The contractor shall generate monthly resource status reports **[Section F, Deliverable 14].** The contractor shall produce monthly/quarterly periodic reports to the DC3 TPOC and Sector Managers from the Management Information System database.

C.6.1.5.2 IT FINANCIAL MANAGEMENT SUPPORT

The contractor shall provide assistance to the DC3 in preparing detailed analyses of business/mission processes regarding financial management and operability. The contractor shall assist with the development, prioritization, and input of the draft DC3 annual Operations and Maintenance (O&M), Research, Development Test and Evaluation (RDT&E) and Other Procurement budgets.

The contractor shall assist with the development, consolidation, and submittal of statistical/financial analysis, financial plans/strategies, budget execution reviews, and unfunded requirements for DC3 Executive Director review and approval. The contractor shall review financial data to identify potential shortfalls and problem areas and report any risks to DC3 management.

The contractor shall assist DC3 in budget planning and execution by reviewing and analyzing financial documentation to assist in justifying on-going program fiscal requirements, identifying and accounting for DC3 program funding, maintaining effective financial controls for the DC3 budget, and providing sound financial recommendations to DC3. The contractor shall track and monitor DC3 appropriated funds, via the Planning, Programming, Budgeting and Execution (PPBE) system. The contractor shall provide assistance in reviewing and ensuring adequate funding is available for DC3 expenditures.

The contractor shall interface daily with functional managers at Secretary of the Air Force / Inspector General's Directorate of Special Investigations (SAF/IGX) and work closely with DoD financial offices/agencies. The contractor shall assist DC3 with supplemental requests in the Planning, Programming, Budgeting and Execution (PPBE) process. The contractor shall coordinate and track all DC3 supplemental requests for annual review and submission.

The contractor shall utilize principles, methods and knowledge of Air Force budget processes to assist in the development, preparation and presentation of programmatic budgeting materials to enable DC3 to fulfill mission responsibilities as a National Cyber Center.

The contractor shall plan, track, analyze, monitor, and report the performance of DC3 financial initiatives **[Section F, Deliverable 15].** The contractor shall develop executive level briefings for presentation to the DC3 Executive Director in defense of the DC3 initiatives **[Section F, Deliverable 16].**

The contractor shall attend meetings for on-going program development and review efforts. The contractor shall focus specifically on Law Enforcement (LE), Counterintelligence (CI), and Information Assurance (IA) program funding and budgeting. The contractor shall assist in preparing responses to inquiries from SAF/IGX and other DoD financial offices.

C.6.1.5.3 PROJECT AND STRATEGIC PLANNING

The contractor shall support DC3 by providing project, strategic planning and coordination support throughout DC3. The contractor shall support the DC3 mission and business goals by assisting the Government in drafting, developing, and writing policies, programs, and procedures to support the success of DC3. The contractor shall gather, research, analyze, and prioritize input on existing and draft policies and procedures related to the governance of D/MM Forensics across the DoD and supporting organizations. The contractor shall document research, analysis, studies, and recommendation in written technical reports; information, point, white, and decision papers; and memorandums for record (MFRs).

The contractor shall be responsible for supporting DC3's participation in the Defense Cyber Operations Group (DCOG) and other Cyber Joint Task Forces (JTF). The contractor shall facilitate DC3 Plans and Policy sponsored meetings, forums, and Working Group sessions, and conferences to include providing logistical support; meeting facilitation; developing and presenting informational briefings; developing and/or analyzing read-ahead material; providing historical records; and analyzing issues resulting from such sessions.

C.6.1.6 DC3 OPERATIONS SUPPORT

The contractor shall provide support to DC3's infrastructure, shared services, and operations, in order to enable DC3's Directorates to meet their mission objectives.

DC3's directorates require the infrastructure and shared services to enable and support their day to day operations. This operational support is delivered by providing security, logistics, financial management, human resources, Directors Action Group, and facilities and infrastructure services. These shared services enable each of the Directorates to focus on delivery of their core mission and maintain a common operational support mechanism. The functions and services mentioned above are not all encompassing as some areas may evolve as the organization evolves.

The contractor shall support and maintain DC3's physical, information, and personnel security program in accordance with AF and DoD policies and regulations. This shall include but is not limited to, managing, implementing, and sustaining DC3's information security programs, overall security programs, information security programs, and physical security program. The Contractor shall work with DC3's security office to maintain security of DC3 facilities, ensure classified information is handled & discarded in accordance with DoD policy, manage DC3's Secure Compartmented Information Facilities, manage personnel clearances, maintain access controls to DC3 facilities, and other security related functions. The Contractor shall also engage with the applicable Air Force, DoD, or other offices with cognizance over a particular security

program or area to maintain DC3 programs up to date and resolve any issues related to DC3 security.

The contractor shall support and maintain DC3's logistics services in accordance with AF and DoD policies and regulations. This shall include but is not limited to, managing, implementing, and sustaining DC3's inventory, material receipt & disposal, mail room services, purchasing, and other logistics functions. The Contractor shall work with and engage AF and DoD offices with cognizance over logistics and procurement to maintain DC3 abreast of the latest guidance and resolve issues that arise related to logistics. The contractor shall support DC3 purchasing by researching alternatives to meet DC3 requirements, tracking orders, supporting Government purchase card holders, and engaging with other government entities to facilitate the purchase of large orders (over $2,500-$25,000).

The contractor shall support and maintain DC3's Financial Management (current year) program in accordance with AF and DoD policies and regulations. This shall include but is not limited to, managing, implementing, and sustaining DC3's financial management program, meeting OSD and AF financial targets, maintaining and generating financial reports execution of appropriated funds in accordance with legislation, and other financial management activities. The Contractor shall work with and engage AF, DoD, and other offices with cognizance over budgets and execution to maintain DC3 abreast of the latest guidance and resolve issues that arise related to DC3 funding. The Contractor shall maintain DC3 Leadership informed on the execution of DC3 funding, provide analysis of spending profiles, and provide full spectrum management and reporting of DC3's current and future budget.

The contractor shall support and maintain DC3's Human Resource Management program in accordance with AF and DoD policies and regulations. This shall include but is not limited to, managing, implementing, and sustaining DC3's human resource management program, maintaining and generating reports and metrics, execution of personnel actions, and other human resource management activities. The Contractor shall work with and engage AF, DoD, and other offices with cognizance over human resources to maintain DC3 abreast of the latest guidance and resolve issues that arise related to DC3 human resources. The Contractor shall keep DC3 Leadership informed on the execution of DC3 personnel actions, provide analysis of HR guidance, provide full spectrum management and reporting of DC3's HR program.

The contractor shall support DC3's Directors Action Group in accordance with AF and DoD policies and regulations. This shall include but is not limited to, managing, implementing, and sustaining DC3's Directors Action Group program, maintaining and generating reports human resource management program, maintaining and generating reports and metrics, execution of activities in support of the Executive Director, tracking of DC3 executive correspondence and reports, and other Director's Action Group activities. The Contractor shall work with and engage AF, DoD, and other offices with cognizance over military performance reports & external engagements to maintain DC3 abreast of the latest guidance and resolve issues that arise related to the DC3 Executive Director. The Contractor shall keep the DC3 Executive Director and the Director of Staff informed on the execution of actions, provide presentation and reports, support for scheduling of meetings, and support other engagements on behalf of the Executive Director.

The contractor shall support and maintain DC3's Facilities and infrastructure program in accordance with AF and DoD policies and regulations. This shall include but is not limited to, managing, implementing, and sustaining DC3's Facilities programs, maintaining and generating reports and metrics assisting in the execution of real property related activities, tracking of facilities projects, and other facilities management and infrastructure activities. The Contractor shall work with and engage AF, DoD, and other offices with cognizance over facilities management and infrastructure to maintain DC3 abreast of the latest guidance and resolve issues that arise related to facilities management. The Contractor shall keep the DC3 Executive Director and the Director of Staff informed on the facilities project status, provide presentation and reports, support for facilities issues, and analysis of alternatives for infrastructure and facilities projects.

C.6.1.7 SUBTASK 1.6 -- TRANSITION IN

The contractor shall ensure that there will be minimum service disruption to vital Government business and no service degradation during and after transition. The contractor shall update their proposed draft Transition In Plan within 5 Government work days of award. **[Section F, Deliverable 12]**

C.6.1.8 SUBTASK 1.7 -- TRANSITION OUT

The Transition Out plan shall facilitate the accomplishment of a seamless transition from the incumbent to an incoming contractor /government personnel at the expiration of the task order. The contractor shall provide a Transition Out plan **[Section F, Deliverable 13]** NLT ninety (90) calendar days prior to expiration of the task order. The contractor shall identify how it will coordinate with the incoming and or Government personnel to transfer knowledge regarding the following:

- Project management processes
- Points of contact
- Location of technical and project management documentation
- Status of ongoing technical initiatives
- Appropriate contractor to contractor coordination to ensure a seamless transition.
- Transition of key personnel
- Identify schedules and milestones
- Identify actions required of the Government.
- Establish and maintain effective communication with the incoming contractor/Government personnel for the period of the transition via weekly status meetings.

C.6.2 TASK AREA 2 -- HELP DESK AND USER SUPPORT (CLIN 0002)

Currently the NMO Help Desk receives over 3000 calls/ requests via the Help Desk Ticket reporting system for assistance annually. It is anticipated that help desk calls/requests will increase by approximately 8-10% annually. The Help Desk receives and answers all telephonic Help Desk calls from all users at three Linthicum, Maryland locations. Helpdesk ticket calls are

normally resolved on the phone if possible or some require technicians to be dispatched to troubleshoot and provide immediate resolution to the problem.

The contractor shall staff and operate the Help Desk for all DC3 computer networks and systems. The contractor shall provide in-person daily technical support services required to support the Help Desk 0600 - 1800 EST on a 12 hours a day, 5 days a week basis.

The contractor shall provide Tier 1 and 2 Helpdesk/Technical support for all DC3 computer networks and systems of various classifications levels to include: Sensitive-but-unclassified (SBU), Secret, Top Secret, SCI, Special Access Program (SAP) and Special Access Required (SAR).

The contractor shall provide Tier 1 Helpdesk/Technical support (initial caller support) for DC3. Tier 1 is the first point of customer contact for network related operational issues. Tier 1 support includes, but is not limited to, requests related to COTS hardware failures, software failures, application questions, installations, relocations, turn-ins, access rights, hardware/software loaners, network communication failures, new user requirements, temporary computer product check-outs, and other computer related requirements.

The contractor shall provide Tier 2 Technical Support (advanced caller support) for DC3 Network users. The contractor shall perform monitoring and troubleshooting of all operational DC3 networks in support of Tier 2 customer and technical efforts. The contractor shall be experienced and knowledgeable with the design and implementation of all DC3 equipment. The contractor shall troubleshoot and resolve Tier 2 DC3 network problems that escalate beyond Tier 1 capabilities. In addition, the contractor shall, as a minimum:

- Identify network problems due to design and implementation constraints;
- Identify and implement workarounds to resolve DC3 network problems;
- Work with DC3 network design engineers on engineering and design issues to develop operationally sound implementations; and
- Develop troubleshooting to enable Tier 1 technicians to efficiently troubleshoot and resolve DC3 network problems.

The contractor shall respond to, and document all network incidents including security and informational requests that result from proactive network monitoring or customer initiated contacts. The contractor shall isolate and document network problems using industry best practice troubleshooting skills, as well as available system and network management tools. The contractor shall use the Help Desk Ticket application as a central repository for technical advice and solutions for network systems, software applications assistance, automatic data processing support, hardware exchange, and repair service support. The contractor shall utilize network management tools to provide efficient, responsive, and rapid problem resolution.

The contractor shall provide Monthly Help Desk Trouble Call Status Reports (TCSRs) **[Section F, Deliverable 17].** The contractor shall provide Help Desk TCSRs that provide relevant data and reports on:

- The analyses/type of trouble calls,
- Unusual patterns,
- Potential DC3 IT/Communications/application problems and proposed resolutions, and
- Unresolved Trouble Tickets,
- Tracking and resolution of service complaints,
- Backup source data,
- The contractor shall also provide a summary status (in spreadsheet format) of all hardware maintenance for each month. This status report should be a part of the Monthly TCSR.

The contractor shall provide end-user training for IT devices; configure e-mail, and all other system operations and features of equipment. The contractor shall assist in identifying training requirements for the Local Area Network Manager (LAN).

The contractor shall collect and report IT Service performance metrics. The contractor, as a minimum shall establish and maintain metrics (subject to Government approval) of the following items, and be prepared to present the findings to DC3 management **[Section F, Deliverable 17]:**

- Total number of queries into the NMO
- Total number of queries into the NMO that result in a trouble ticket
- Total number of queries that are resolved during initial contact
- Total number of queries resolved by the NMO
- Total time to complete (resolve) the trouble ticket

The contractor shall respond to customer Help Desk requests within four (4) hours and it is desired to resolve 90% of trouble tickets within 24 hours. The contractor shall provide supporting documentation to be validated by the DC3 TPOC for those requests beyond the desired response period due to unusual circumstances. The contractor provided help desk support shall track through to completion all tier 1 and 2 help desk tickets.

C.6.3 TASK AREA 3 – PROVIDE SYSTEMS OPERATION SUPPORT (CLIN 0003)

The contractor shall support the Network Management Office (NMO) in the operation, administration, design, installation, configuration and maintenance of its computer, information and communications systems operation that enable DC3 to accomplish assigned missions.

C.6.3.1 SUBTASK 3.1 -- NETWORK SUPPORT

The contractor shall provide effective, efficient, secure, and reliable information network services for DC3. The contractor shall assist in the development, management and maintenance of all DC3 computer networks and all associated network resources.

The different types of information handled by DC3 necessitate the use of different computer networks. The contractor shall maintain, support and troubleshoot several classified and unclassified networks to include: DC3 Enterprise Network (NIPRNET), Secret Internet Protocol

Router Network (SIPRNET), Joint World-Wide Communications System (JWICS) Network, the LIMS/CIMS Network, the Examiner Network, Covered Accounts Network, and other networks are required.

The contractor shall provide proactive and reactive management of resources by monitoring and controlling networks, available bandwidth, hardware, and distributed software resources. The contractor shall respond to detected security incidents, network faults (errors), and user reported outages at the time of customer identification. The contractor shall document, record and report all network incidents **[Section F, Deliverable 19].**

The contractor shall maintain all addressing schema for all infrastructure of the enterprise, modify switch, router, and hub configurations to ensure optimum network performance. The contractor shall configure and maintain Access Control Lists (ACL's) to grant/restrict network access to authorized users and configure desktop systems utilizing the Dynamic Host Configuration Protocol (DCHP). The contractor shall maintain domain name system (DNS) servers for internal and external name resolution.

The DC3 operates Virtual Private Network (VPN) on unclassified network enterprises. The contractor shall maintain a working knowledge of the VPN and the Internet Protocol Security (IPsec) that enables VPNs. The contractor shall perform routine network troubleshooting of vendor specific VPN devices.

The contractor shall configure, operate, and maintain enterprise network management systems and provide necessary backup of such systems to include server hardware, operating systems and applications. The contractor shall be responsible for collecting and archiving the data necessary to conduct detailed infrastructure mapping and analysis, producing time-sensitive displays and threshold alerts, and developing course of action scenarios.

The contractor shall develop and maintain a network back-up recovery plan **[Section F, Deliverable 21].** The back-up recovery plan shall include a listing of required equipment, timelines, and training (on the network back-up recovery plan) associated with the solution.

System availability and connectivity is critical to the day-to-day operations of DC3. It is desired that network operations and systems administration will maintain monthly 99.5% network/systems availability on all DC3 internal networks unless unusual circumstances beyond the contractors control occur. The contractor shall document these circumstances by submitting an exception request within one week of an incident to request that the Government determine if a situation is beyond the contractor's control. The contractor shall monitor, maintain, and report monthly system availability, up-time and down-time.

C.6.3.2 SUBTASK 3.2 -- SYSTEM AND APPLICATION ADMINISTRATION SUPPORT

The contractor shall provide daily system operational administration services for DC3 systems and applications. NMO's current IT is composed of servers, personal computers (PCs), laptops, printers, scanners, routers, network devices and tools supporting the DC3 network infrastructure.

The contractor shall conduct day-to-day operations, trouble-shooting, transitions, installations, maintenance, conversions, cutovers and sustainment of all IT components. Operational system and application administration support services include:

- Establish, monitor and maintain all computer and network accounts
- Adding, changing, or deleting user accounts, mailboxes, passwords, and file access rights
- Document and update all accounts and locations **[Section F, Deliverable 20]).**
- Maintaining an up-to-date listing of user accounts, e-mail accounts, passwords, software licenses, systems file directories and system/network accreditation documentation.
- Administering and monitoring password changes by NMO computer security regulations
- Creating, allocating, monitoring, and restoring data files and space
- Operating, trouble-shooting, and repairing server software malfunctions
- Executing emergency recovery plans during major server crashes ensuring minimal server disruption.
- Back-up and recovery
- Proxy Administration
- Conduct analysis of network characteristics to include traffic, connect time, transmission speeds, packet and modifications to network and system components
- Operate, maintain and trouble-shoot video teleconferencing hardware and software
- Maintain the Global Address List, MS Active Directory and other network directory services.
- Manage internet and intranet web servers, remote Access Security Services and maintain the DNS server.
- Maintain and monitor standardized file storage directory structures.
- Establish, maintain, and monitor print servers.
- Establish and administer Oracle™ and Microsoft™ database servers
- Establish and administer Microsoft™ Exchange Servers
- Establish and administer Microsoft™ SharePoint Servers

The contractor shall act as the intermediary between the end-user workstation providing expert system administration, technical support, security, administrative control, and application services for all operational systems.

C.6.3.3 SUBTASK 3.3 – ENTERPRISE ARCHITECTURE (EA), AND CONFIGURATION MANAGEMENT (CM)

The contractor shall develop and maintain DC3 EA documentation to DoD Architecture Framework (DoDAF) standards.

The contractor shall conduct configuration management planning and implementation services. The contractor shall install and configure Windows, Apple, and Linux-based operating systems.

The contractor shall be responsible for requirements analysis, evaluation, and design of the IT architecture environment for DC3. The contractor shall maintain a current network architecture and configuration design for all DC3 networks.

The contractor shall support the installation and configuration of network servers, routers, and other peripherals. The contractor shall be responsible for Configuration Management design, architecture, and Computer-off-the-shelf (COTS)/Government-off-the-shelf (GOTS) software and hardware integration to include, but not limited to describing provisions for configuration identification, configuration of requirements documentation, design documentation, software and related documentation.

The contractor shall be responsible for configuration change control, configuration status accounting, and configuration audits. The contractor shall regulate the change process so that only approved and validated changes are incorporated into product documents and related software. The contractor shall track and report all configuration management problems and support software quality assurance process audits.

The contractor shall evaluate, implement, and configure hardware and software to ensure Air Force Information Protection (AFIP) and DOD policies are enforced and safeguards are active.

The contractor shall configure test beds to conduct testing on DC3 networks; record and analyze results; and provide recommendations for improvements of the products/systems tested. The contractor shall encode, debug, and test software applications to meet established operational and system requirements using industry standard products such as programming languages and tools as required.

C.6.3.4 SUBTASK 3.4 -- REPAIRS, UPGRADES, AND INSTALLATION

The contractor shall support all DC3 computer/communications infrastructure, including D/MM forensic workstations, and make recommendations to the Government for upgrades, equipment replacement, repairs, changes, additions, and removal of parts of this infrastructure.

The contractor shall perform general server and Automated Data Processing Equipment (ADPE) repair and servicing. The contractor shall support the maintenance of all DC3 mission critical equipment to include: Computers, printers, scanners, laptops, and other IT systems to ensure successful operations of the DC3 network systems and related equipment.

The contractor shall notify the Government of all necessary required changes, additions or removals from the existing system and obtain concurrence before any changes, additions or removals are performed. The contractor shall document all repairs, changes, additions or removals in the summary status included in the TCSR.

The contractor shall install and remove hardware, software and network components. The contractor shall install, modify and maintain DC3 switches, routers, hub configurations and cabling comprising the DC3 networks. The contractor shall install and manage video teleconference equipment as well as schedule and facilitate video teleconferences.

The contractor shall conduct technical testing on existing and newly procured NMO systems, subsystems and applications. The contractor shall evaluate communications hardware and

software, troubleshoot problems, and provide technical expertise for optimal performance of equipment. The contractor shall recommend additional hardware and software tools which could improve the systems.

C.6.3.5 SUBTASK 3.5 -- IT ASSET MANAGEMENT

The contractor shall be responsible for the tracking, receiving, distributing and accounting for DC3's hardware and software inventory. The contractor shall be responsible for maintaining a complete inventory of all major hardware components and recording serial numbers. The contractor shall maintain and update a software library accounting for all software, licenses, and issuance data.

The Contractor shall determine, document, and regularly update the total cost of operations (TCO) for each DC3 network

The contractor shall track the life cycle of all hardware, software, and communication equipment, from user request for the equipment, through installation, maintenance, and surplus and disposal. The contractor shall document and submit a Report of Survey to the appropriate AF Logistics Office if any accountable items are lost or damaged. The contractor shall develop and maintain an ADPE program for tracking and managing DC3 owned IT assets.

The contractor shall conduct market research on commercial computer and software products in support of D/MM forensics and associated technology. The contractor shall analyze, present findings and recommendations to DC3 to determine the most efficient, effective and overall best value.

The contractor shall prepare required purchase documents, work statements, justifications, acquisition plans and coordination packages for the purchase and maintenance of computers, computer equipment, and other related products in support of the DC3 mission.

C.6.3.6 SUBTASK 3.6 -- INFORMATION PROTECTION (IP) AND INFORMATION ASSURANCE (IA)

The contractor shall be responsible for maintaining extensive security protection of all DC3 data and systems. The contractor shall serve as the point of contact (POC) for DC3 IT infrastructure security and related issues. The contractor shall provide technical leadership to maintain the integrity and privacy of DC3 mission information systems through separate IP and IA functions.

The contractor shall provide IP services to include active security vulnerability assessment, implementation, and monitoring of all computer systems and network infrastructure. The contractor shall perform vulnerability/risk analyses of computer/network systems and applications during all phases of the system development life cycle.

The contractor shall assist in eliminating the threat of network intrusion by proactively probing network defenses to identify vulnerabilities to include administering network scans as required.

The contractor shall update servers as new security vulnerabilities are released, periodically rescan servers to ensure the latest security updates are enforced, ensure Information Assurance Vulnerability Alert (IAVA) and Tactical Computer Network Operator (TCNO) compliancy, and provide real-time protection from any threats of active files using anti-virus tools. The contractor shall operate and maintain firewall(s), web proxy, caching servers, and e-mail gateway servers to protect DC3 information resources from internal and external threats. The contractor shall ensure all current network security tools and patches are implemented across all internal DC3 systems. The contractor shall conduct quarterly security scans of computer/network systems and advise the Government of potential computer security concerns and problems along with recommendations for solutions.

The contractor shall analyze information protection-related issues and provide engineering, technical and management solutions. The contractor shall design, develop, implement and support the integration of information protection solutions and technologies into computer/network systems and applications with particular attention to protocols, interfaces, and system design; technical information about the DC3's mission goals and needs; existing security products; ongoing advances in computer security; and security requirements for operational systems as well as systems under development.

The contractor shall develop/maintain measures and controls to protect the DC3 networks from denial of service, unauthorized access, and modification of data and destruction of DC3 networks, network components or information processed on them. The contractor shall maintain, support, enhance and document a comprehensive DC3 IT Information Assurance (IA) program. The contractor shall establish and maintain IA policies, procedures and awareness.

The contractor shall perform information protection functions for networks and systems. The contractor shall test computer/network systems and applications for the following:

- Ease of unregulated entry
- Systems resources denial
- System information corruption
- Unlawful use of system resources
- Vulnerability to electronic disruption.

The contractor shall report and document all identified system attacks to the DC3 TPOC.

The contractor shall provide support related to Communications Security (COMSEC). The contractor shall document receipt, custody, issuance, transmittal, storage, accountability, classification, and destruction of all Classified Material. The contractor shall maintain logs and journals to comply with AF security, regulatory and policy guidelines. The contractor shall be responsible for maintaining and updating all Secure Telephone Equipment (STEs), records, and self-inspection programs concerning Classified Material.

The contractor shall ensure all systems and equipment are operated and maintained in accordance with DoD, DISA, USAF and AFOSI security guidelines, directives and updates. The

contractor shall ensure all security policies are within the limits of existing architecture and software capabilities.

The contractor shall ensure the DC3 network and systems are 100% in compliance with applicable DoD and USAF directives for Network & Computer Security.

C.6.3.7 SUBTASK 3.7 – BUSINESS PROCESS MANAGEMENT (BPM) AND TECHNICAL DOCUMENTATION (TD) DEVELOPMENT

The contractor shall provide BPM services to review, improve, maintain, and document DC3 business processes. All DC3 business processes will be identified and reviewed on a recurring basis. Processes will be documented to Integrated Definition (IDEF) modeling and/or Capability Maturity Model Integration (CMMI) standards.

The Contractor shall utilize the results of these BPM efforts to clarify IT requirements and to document DC3 Standard Operating Procedures (SOPs), policies and directives.

The contractor shall develop, maintain, and implement external and internal network Standard Operating Procedures (SOPs)/user manuals, policies and directives to include operations, maintenance and sustainment in the DC3 NMO environment. The contractor shall interpret DoD and Air Force Instructions, AFOSI Supplements, and incorporate network and system requirements the SOPs. The contractor shall ensure all systems and software are documented and controlled in accordance with the DC3 Standard Operating Procedures (SOPs).

The contractor shall prepare technical manuals, edit documents/publications, develop graphic documentation and technical operation/maintenance engineering drawings, and execute configuration management/storage management of documentation relating to DC3's infrastructure.

The contractor shall draft procedures, document and design network configurations including the diagramming of all equipment.

The contractor shall develop, prepare, edit, modify, catalog and manage IT infrastructure technical documentation regarding programs and integrated systems.

The contractor shall ensure 100% compliance in accordance with AFI 33-114, Communications and Information Software Management.

C.6.3.8 SUBTASK 3.8 - IT TECHNICAL EXPERTISE AND MODERNIZATION

The contractor shall provide technical expertise to support the implementation and modernization of DC3's client, server, and network systems as well as the applications they support. The contractor shall conduct the evaluation, design, and development of the data networking and telecommunications systems, both hardware and software. The contractor shall provide technical direction and engineering expertise for communication systems and

infrastructure activities, including planning, designing, and implementing communications infrastructure requirements for the DC3 buildings and systems.

The contractor shall conduct market research and evaluate emerging technologies with respect to the DC3 IT infrastructure. The contractor shall interface with internal and external stakeholders to determine communications infrastructure needs.

The contractor shall conduct cost and benefit analysis on network equipment and recommend system upgrades to the DC3 TPOC as part of life cycle replacement.

The contractor shall assist with concept development, project design, scheduling, funding, budget support, implementation and development of all system and building renovation/upgrade projects. The contractor shall brief all project proposals monthly and provide updates to DC3 management on the status of such projects.

The contractor shall assist in ensuring adequate and appropriate planning, space allocation and utilization requirements is provided to building planners in building communication spaces and media pathways to meet DC3 standards. The contractor shall assist in determining requirements and coordinating building upgrades and renovation projects to adequately meet DC3's mission to provide state of the art forensic computer support.

As new technologies become available and beneficial to the users, the contractor shall be responsible for the evaluation, testing, implementation, and maintenance support for those enhancements.

C.6.3.9 SUBTASK 3.9 – WEB, PORTAL, AND CONTENT MANAGEMENT SYSTEM (CMS) DEVELOPMENT AND MANAGEMENT

The contractor shall be responsible for overall DC3 internet and intranet web-sites, collaborative portals and CMSs across all network domains. The contractor shall provide administrative, development, and technical management of all facets of the DC3 managed web-sites portals, and CMSs.

The contractor shall develop and implement overall policies/procedures for web-site, collaborative portal, and CMS structure, format, usage, and promote participation in the use of these capabilities activities. The contractor shall establish organizational standards for DC3 managed Web sites. The contractor shall design consistent methodologies for the development of internet resources across the organization.

The contractor shall conduct periodic reviews of DC3 web sites, portals and CMSs to keep content up-to-date and ensure compliance with established standards. The contractor shall ensure compliance with DoD and USAF standards for Web services.

The contractor shall perform short and long-term strategic planning of the integrated internet resources for DC3. The contractor shall coordinate, integrate and manage information contributed to the web-sites, portals, and CMSs to include: establishing template formats,

logistical structures of web-pages, guiding and assisting contributors with editorial and publishing related issues. The contractor shall review web content and identify issues that may present potential legal problems to include: trademark/copyright infringement, libel, controversial issues.

The contractor shall analyze, develop, implement, maintain, document, and modify web-based applications. The contractor shall perform continual evaluations of web-site, portal, and CMS software and hardware to ensure continued and future effectiveness and efficiency of these capabilities. The contractor shall encode, debug, and test web software applications to meet established operational and system requirements.

The contractor shall evaluate, recommend and administer internet search systems and programs, design interactive authoring language forms to support on-line information exchange.

The contractor shall maintain the World Wide Web (WWW), NIPRNET, SIPRNET, DFI Portal and JWICS web-sites and content. The contractor shall design and create web pages and templates in accordance with Government requirements/standards.

The contractor shall centralize the intranet capabilities for maintenance and access by all of DC3 personnel.

The contractor shall provide and organize the basic source material, including applicable designs, technical information, and maintenance for the DC3's web content. The contractor shall interface with DC3 personnel to research and interpret technical information in order to create, maintain, and reproduce web content.

The contractor shall ensure 100% compliance in accordance with Applicable DoD and USAF directives.

C.6.3.10 SUBTASK 3.10 -- DATABASE MANAGEMENT SUPPORT

The contractor shall provide database installation, configuration and management.

Current DC3 databases include Center's Information Management System (CIMS)

The contractor shall provide the overall management, support, and maintenance of the CIMS database. The contractor shall be responsible for ensuring CIMS data integrity.

The contractor shall maintain the CIMS (STARLIMS) database and ensure the accuracy and currency of all information contained in the database. The contractor shall provide the following support for maintaining the CIMS databases:

- **Data Currency and Updates:** The contractor shall ensure databases contain the most current information available. To maintain currency, the contractor shall establish procedures and tools for updating the database with information that is periodically refreshed and for timely review and update of information that is not periodically

published. Preferably, the contractor shall update data automatically, if consistent with the need for security and data integrity. If not possible, the contractor shall use manual, automatic, or a combination of methods to update the data.

- **Database Structure Modification:** The Contractor shall modify the information contained in the database as directed by the Section Chief.

- **Accessibility:** The contractor shall ensure that information from the databases will be accessible to users as determined by the Section Chief using documented instructions provided by the contractor. The contractor shall develop and administer security procedures to ensure only valid users have access to data and data modification.

C.6.3.11 SUBTASK 3.11 - TELECOMMUNICATIONS/PHONE SYSTEM MANAGEMENT

The contractor shall provide overall support to DC3's telephone, telecommunications systems, and Secure Telephone Equipment (STE). The contractor shall provide day-to-day technical administration of the phone system, perform scheduled and non-scheduled maintenance, coordinate repair actions, and verify telecommunications circuits are active and available for use. The contractor shall monitor the performance of telephone sets, voicemail systems, modems, fiber optic cables, telephone switching units, and data circuits.

The contractor shall provide end-user training for telephone devices; configure voice-mail, and all other phone system operations and features of the equipment.

It is desired that the contractor shall ensure the phone system will maintain 100% availability. The contractor shall maintain 100% phone system availability unless prevented by unusual circumstances beyond the contractor's control. The DC3 TPOC will determine if a situation is beyond the contractor's control.

C.6.3.12 TASK 3.12 –Evidence Custodial Support (DCFL)

The contractor shall assist the evidence custodian in ensuring an effective evidence program is maintained and provides support services for all evidence entering and exiting DCFL.

All contractor personnel assigned to the Evidence Room will be trained to handle evidence in accordance with DCFL and DoD policies. Upon completion of the training program, personnel will be required to pass a written test to work in the Evidence Room.

The contractor shall follow established procedures outlined in the American Society of Crime Laboratory Directors/Laboratory Accreditation Board (ASCLD/LAB) International Program (ISO 17025) Accreditation and AFOSI instructions for incoming evidence into the laboratory for media analysis. The contractor shall receive, inspect and administratively process all incoming evidence, packages and freight deliveries into the laboratory. Some items received maybe large and the contractor shall be capable of handling heavy objects.

The contractor shall establish chain-of-custody document for all evidence to document the transfer of the evidence within DCFL.

The contractor shall assist with logging in all evidence received by the DC3 in accordance with AFOSI evidence handling procedures and properly maintain the computerized evidence program. The contractor shall update and maintain the DCFL Evidence Handling and Control Log and ensure it is current.

The contractor shall identify, photograph, store, and ensure all evidence is properly marked, tracked and processed. The contractor shall update received evidence into the DCFL Evidence Tracking System (ETS) and log new cases into CIMS.

The contractor shall seal and safeguard evidence and media in accordance with current DCFL SOPs, ASCLD ISO 17025 and AFOSI instructions to include AFOSI Manual (AFOSIMAN 71-118) and the AFOSI Crime Scene Manual (AFOSIMAN 71-124). The contractor shall assist in resolving evidence control problems.

The contractor shall create, update, maintain case folders containing all required forms and supporting documentation for the case.

The contractor shall be responsible for issuing evidence to corresponding examiners. The contractor shall ensure the integrity of the evidence is maintained by ensuring all evidence is signed in and out. The contractor shall monitor and control the evidence in all aspects of laboratory operations and shall conduct reviews of all incoming and outgoing evidence chain-of-custody documents.

The contractor shall support a semi-annual inventory of maintained and stored evidence. The contractor shall document all stored evidence and verify evidence is logged into the ETS.

The contractor shall be responsible for returning all evidence to the owning agency when the imaging and extraction process is complete. The contractor shall support the tracking and monitoring of all related shipping costs identifying all costs to the DC3 Financial Manager for review.

C.6.3.13 SUBTASK 3.13 -- DATA IMAGING AND EXTRACTION (I&E) SUPPORT

The contractor shall prepare and perform forensic imaging and extraction on computer digital devices and storage media such as hard drives, removable media, and optical removable media (in support of all DoD missions and investigations) to include but not limited to,

- Hard Disk Drives; floppy diskettes, ZIP drives, and similar removable disks;
- Data Tapes, Media Cards, Thumb Drives, CD ROMS, and DVDs;
- Personal Digital Assistant Devices and Cell Phones;
- Digital Audio and Video Recording and Storage devices, Cameras, and Game boxes.

The contractor shall be required at times to provide on-site imaging and extraction at specific evidence sites and alternate operating locations.

NOTE: SOME OF THE DATA IMAGES EXAMINED WILL CONTAIN EXTREMELY OFFENSIVE, OBJECTIONABLE AND/OR SEXUALLY GRAPHIC MATERIAL, WHICH MAY BE DISTURBING.

The contractor shall perform forensic imaging and extraction of digital information in support of examinations of computers and media generated by computers to develop evidence/intelligence information. The contractor shall be required to process approximately 1,300 requests per year with a potential increase of 40% per year. Currently the "average" request is approximately 152GB of data on fifteen pieces of media. The estimated time required for data imaging and extraction is less than ten (10) days. The amount of time required is dependent upon the DCFL Case Suspense Calculator and determination of the DCFL Government Director of Operations (DO). The size and complexity of each individual request is taken into consideration including the type, format and condition of the media to be imaged in order to accurately estimate the reasonable suspense.

The contractor shall be responsible for extracting and duplicating forensically sound images of the media utilizing DCFL approved and specified imaging tools. Once the evidence or original media is extracted and duplicated, the contractor shall be responsible for archiving all image files to an appropriate storage media.

The contractor shall process forensically extracted data through Government provided software utilizing the hardware provided by the Government and approved SOPs.

The contractor shall record, document and maintain written notes throughout the duplication process. The contractor shall process evidence and all associated corresponding administrative paperwork to include CIMS input and all other required forms in a proper and timely manner. The contractor shall document and report any noted evidence discrepancies. The contractor shall follow the procedures and methods outlined in the DCFL SOP.

The contractor shall be responsible for the repair and recovery of data from damaged media. The contractor shall employ specialized techniques of Hard Drive Repair, Disk Splicing and Disk resurfacing and produce restored copies of the suspect media for examination.

The contractor shall participate, present and provide input at briefings, meetings, conferences, panels, boards, seminars, working group sessions, technical exchanges and public forums on cyber crime and forensic-related IT media imaging and extraction as needed.

C.6.3.14 TASK 3.14 – D/MM FORENSIC EXAMINATION AND ANALYSIS SUPPORT

The contractor shall provide D/MM forensic examination and analysis support for all types of electronic media in support of criminal, fraud, counter intelligence, cybersecurity, data recovery, terrorism, and safety investigations. Investigations may include homicide, child pornography,

identity theft, counterfeiting, misconduct, terrorism, intrusions, contractor fraud and misuse of Government property. The contractor shall be required at times to provide on-site examination and analysis at specific evidence sites.

NOTE: SOME OF THE DATA IMAGES EXAMINED WILL CONTAIN EXTREMELY OFFENSIVE, OBJECTIONABLE AND/OR SEXUALLY GRAPHIC MATERIAL, WHICH MAY BE DISTURBING.

C.6.3.14.1 SUBTASK 3.14.1 -- EXAMINATION SUPPORT

The contractor shall provide basic and advanced forensic analysis support of digital media.

The contractor shall assist with planning, organizing and supporting an approach to obtain useful forensic information from the evidence submitted to DC3 while meeting the requirements established by agency regulations, federal law, the Uniform Code of Military Justice, DC3 SOPs, DC3 Quality Assurance (QA) guidelines, and the DC3 Personnel Handbook.

The contractor shall receive, review and maintain the integrity and proper custody of the evidence. The contractor shall identify and report any discrepancies in receipt of the evidence to the Evidence custodian **(as needed [Section F, Deliverable 22]).** The contractor shall ensure forensic processes; handling and hardware utilized are designed to safeguard all submitted evidence.

The contractor shall ensure all facility physical security, network security and safety requirements are followed in regards to forensic examinations and analysis.

The contractor shall provide substantive analysis of computers and media generated by computers to develop evidence. The contractor shall conduct an examination utilizing only DCFL approved procedures, hardware, and software as specified in the DCFL Currently Approved Configuration Item (CI) documents.

The contractor shall perform forensic analysis on computer magnetic storage media to develop evidence/intelligence information in support of DoD investigations.

The contractor shall conduct specialized forensic examinations of audio/visual media to develop evidence/intelligence information in support of DoD investigations.

The contractor shall conduct advanced and future D/MM forensics by utilizing Large Data Sets, Loss of Control, Steganography, Global Positioning (GPS), Peer-2-Peer Technologies, Malicious Code Analysis, Data Visualization/Data Mining, Metadata Retrieval/Analysis, Project Vision (Video and Image Retrieval/Analysis), Public Key Infrastructure (PKI), Biometrics, Encryption Detection and Defeat, Hard Drive Repair, Data Recovery from Damaged Advanced Media, Operating System (OS) Reconstruction, Password Cracking, Damage Assessment techniques along with GOTS and COTS software.

The forensic examination performed by the contractor shall normally include verification and comparison of the forensic image files, examination for the presence of malicious logic such as viruses, Trojans, worms, etc., examination of media for deleted files and folders, documenting active and recovered deleted files, analysis for misnamed files, conducting word searches and analysis for relevant hardware and software configuration information.

The contractor shall assist in data recovery to determine the most appropriate method of protecting original evidence and recovering deleted, erased, hidden, and encrypted data.

The contractor shall write concise, comprehensive and accurate written notes throughout the examination process. The contractor shall develop a complete D/MM Forensic Analysis Report (DFAR) upon completion of the examination **([Section F, Deliverable 23]).** The report shall be written in Microsoft Word (or appropriate) and document a complete examination. The contractor shall ensure the report is scientifically valid, readable, and compliant with all DC3 procedures.

The contractor shall perform technical peer reviews and feedback of other examiners cases. The technical peer review shall include reviewing other examiners reports for scientific validity, readability, and administrative compliance with all procedures.

The contractor shall be required to present findings of their examinations in Military, Federal, State and/or local courts of law. The contractor shall provide expert/witness testimony of evidence findings, analysis, and examination. The contractor shall be prepared to provide forensic testimony on short notice requests. The contractor shall be required to travel to CONUS and OCONUS court proceedings to provide testimony.

The contractor shall assist the DC3 Attorney Adviser in providing legal review, analysis and examination of all documents submitted and created by DCFL regarding forensic examinations. The contractor shall compare the information against the Fourth Amendment and Electronic Communication Privacy Act standards when making legal recommendations for disposition concerning forensic information and examinations.

The contractor shall assist the DC3 Attorney Adviser in preparing examiners for testimony in a court of law. The contractor shall develop charts and illustrations to support the DCFL examiner in testimony at trial. The contractor shall establish, maintain, and facilitate a mock trial program with DCITA to assist examiners in preparing to present findings in a court of law.

The contractor shall participate, present and provide input at briefings, meetings, conferences, panels, boards, seminars, working group sessions, technical exchanges and public forums on cyber crime and D/MM forensic examination and analysis as needed.

The contractor shall support in developing an initial pilot that will perform cross collection analysis to determine useful data and content across a number of National Media Exploitation Center (NMEC) databases.

C.6.3.14.2 SUBTASK 3.14.2 -- QUALITY ASSURANCE MANAGEMENT AND DEVELOPMENT

The contractor shall provide assistance to DCFL in maintaining, updating and managing the Quality Assurance Program (QAP) as documented in the American Society of Crime Laboratory Directors/Laboratory Accreditation Board (ASCLD/LAB) ISO 17025. The contractor shall support the maintenance, updating and management of the DCFL Quality Manual and the Personnel Quality Assurance Program, defining methodologies and documenting policies, procedures and protocols within DC3.

The Government has provided initial performance metrics in a Draft Quality Assurance Surveillance Plan (QASP) in Section J Attachment N. The contractor shall, maintain the DCFL QAP to include performance metrics to measure the lab's effectiveness, formal and informal reviews of analyses, methods to ensure quality and customer satisfaction.

The contractor shall support and implement goals, milestones and objectives mandated by the ASCLD/LAB ISO 17025. The contractor shall assist the DC3 TPOC in ensuring the QAP is run in accordance with the Quality Manual to ensure accreditation of the facility by the ASCLD/LAB ISO 17025.

The contractor shall support a project plan to guide the metrics program. The project plan shall present a structured approach to maintaining and implementing the metric program. The contractor shall develop and maintain the most efficient organizational structure for implementing and managing the program. The plan shall include the overall methodology for identifying, gathering, and analyzing the measures as well as identifying participants and stakeholders, milestones/schedule and deliverables.

The contractor shall work with each DCFL Section's Chief to identify the objectives and core processes they support to ensure inter-connectivity and joint accountability of the strategy across DCFL and DC3. The contractor shall assist each Section's Chief to refine their existing missions and sub-organizational models to reinforce how they would support the overall mission and vision. The contractor shall document **[Section F, Deliverable 24]** the following outcomes:

- Vetted strategy with vision, mission, goals and objectives
- Core processes and roles and responsibilities assigned to each organization's team members
- Initial, high-level measures for assessing the organization's success
- Organization direction and strategy
- Prioritized list of strategic objectives
- Documented short-term and long-term goals.

The contractor shall assist the DC3 TPOC with the development and maintenance of the DCFL's and/or DCCI's Procedures Manuals. The contractor shall provide input, strategy and guidance on updating, enhancing and developing procedure manuals for DC3.

C.6.3.14.3 TASK 3.14.3 DCFL TRAINING REQUIREMENTS AND DEVELOPMENT

To remain on the cutting edge of advances in D/MM forensic technology, DCFL personnel require continual training. The contractor shall support DCFL by monitoring, updating and tracking all DCFL personnel training through completion to maintain currency and adherence to the QAP.

The contractor shall assist the DC3 with the establishment and maintenance of a database containing all DCFL personnel credential information to include: Examiners and forensic support staff working in the DC3.

The contractor shall track and monitor education and training, court appearances and testimony, examinations performed, and peer reviews performed. The contractor shall assist with the creation and population of the credentials database**..**

The contractor shall query credential data and create a quarterly report on certification and training status **[Section F, Deliverable 25]**. The Credentials Management Database shall categorize and track D/MM Forensic Examiners' proficiency levels as described in the DCFL Employee handbook.

C.6.3.15 SUBTASK 3.15 FORENSIC TRAINING PROGRAM

The contractor shall assist DC3 with establishing and maintaining requirements for a D/MM Forensic Examiner Proficiency Testing Program.

The contractor shall incorporate test results into the Personnel Quality Assurance Program and advise the TPOC on future actions for proficiency testing.

The contractor shall assist in developing and maintaining a remedial action plan to ensure all Forensic Examiners successfully complete proficiency tests as required by the QAP to perform forensic work in DCFL.

C.6.3.16 SUBTASK 3.16 FORENSIC MENTORING PROGRAM

The contractor shall assist the DC3 with the establishment and management of a D/MM forensic examiner mentoring program to assist in the training of all new DCFL employees in accordance with the DCFL Employee handbook and DC3 Standard Operating Procedures (SOPs). The contractor shall ensure all new employees are assigned a mentor to provide guidance through site-specific policies, initial tasks and training. The contractor shall document the effectiveness of the mentor program and provide input on strategies to improve the new employee transition in DCFL.

C.6.3.17 TASK INTAKE & OUTREACH SUPPORT (DCFL)

The contractor shall support inbound customer service inquiries and assist in resolving errors in customer service requests. The contractor shall support review and validation of DCFL forensic examination requests for minimum requirements. The contractor shall support Intake in identifying potential conflicts with laboratory workflow or policy. The contractor shall provide inputs on strategies to develop customer service capabilities.

C.6.4 TASK AREA 4 – PROVIDE DCCI OPERATIONAL SUPPORT

The contractor shall assist DCCI in providing legally and scientifically accepted standards, techniques, methodologies, research, tools, and technologies on digital forensics to meet current and future threats. The contractor shall assist DCCI with pioneering digital forensic tools, processes and procedures to ensure DC3 remains on the leading edge of the discipline. The contractor shall assist DCCI in managing the planning, programming, and execution of program and infrastructure requirements linked to advancing digital forensic research, development, test, and evaluation efforts.

C.6.4.1TASK 4.1 – RESEARCH AND DEVELOPMENT ASSISTANCE

The contractor shall assist with the planning, establishment and maintenance of research and development of computer forensics development efforts. Once developed, these solutions are inherent to the Government.

The contractor shall assist DCCI with creating, reviewing, and prioritizing requests. The contractor shall create and maintain a methodology for tracking and maintaining the status of all requests and provide a quarterly status report **[Section F, Deliverable 26]** outlining upcoming research and development.

The contractor shall ensure all established requirements requests are in line with agency regulations, federal law, the Uniform Code of Military Justice, DC3 Standard Operating Procedures and Quality Assurance guidelines, and the DC3 Personnel Handbook in developing computer software and performing forensic tests of computer forensic software. The contractor shall provide a written analysis of all requests that are outside the scope or problematic to such regulations **[Section F, Deliverable 27]**.

The contractor shall assess research requests, ensure validated user requirements and produce relevant/useful products in a timely manner. The contractor shall develop a project plan, including milestones, to address the requirements. **[Section F, Deliverable 28].** The contractor shall review requests for existing solutions as well as commonalities with other solutions and document those identified commonalities.

Dependent upon the requirements of the request, the contractor shall research, design, and develop software, employing tools, processes, and procedures in keeping with guidelines specified in the DC3 Software Development Process and Procedures (March 2011).

The contractor shall provide an electronic Weekly Activity Report (WAR) to include updates of status and progress of current and upcoming Form 10 requests. The contractor shall track requests through the appropriate tracking software and identify time accrued on particular requests. The contractor shall prepare briefings on the progress, outcome or evaluation of requirements. **[Section F, Deliverable 29].**

Dependent upon the nature of the requirement, the contractor shall gather, analyze, and prioritize existing research and informal studies to identify and collect publicly available information/tools to support and enhance DCCI research and development activities leading to forensic technical solutions. Based on findings, the contractor shall provide written analysis and recommendation of further DCCI research and development ideas/strategies as needed. The contractor shall document research, analysis, studies, and recommendations in written technical reports; information, point, white, and decision papers, or memorandums for the record(MFRs).

The contractor shall participate, present and provide input at briefings, meetings, conferences, panels, boards, seminars, working group sessions, technical exchanges and public for/on cyber crime and forensic-related IT media research and development.

C.6.4.2 TASK 4.2 – TESTING AND EVALUATION ASSISTANCE

The contractor shall assist DCCI with the planning, establishment, and operations for tests and evaluations of computer, computer forensic processes, hardware and/or software in compliance with the DC3 Test and Evaluation Standard Operating Procedures. The components of which include, but are not limited to: creating test data sets, developing a test plan, carrying out the tests in a scientific manner, and generating reports outlining the test findings along with any anomalies and/or observations which could prove useful to digital forensic examiners when employing the given tool or procedure. The contractor shall also prepare Project Status Review presentations which serve to document the steps undertaken by the contractor to validate that a given digital forensic tool, process, or procedure is forensically sound.

Performance at off-site locations shall be approved in advance by the TPOC in coordination with the DCCI Director.

C.6.4.3 TASK 4.3 — D/MM FORENSICS INFORMATION (DFI)

The contractor is also responsible for the distribution of accumulated D/MM forensics knowledge to be release back to the D/MM forensics community to aid Law Enforcement (LE) and the U.S. Government. The methods of information disbursement are primarily focused on the Nation Repository for D/MM forensics Information (NRDFI) portal, which is managed in part by Oklahoma State University (OSU) and regularly published DFI Bulletins.

The contractors supporting the DFI team shall be responsible for:

- DFI Bulletin
- National Repository for D/MM forensics Information (NRDFI) Portal
- DC3 Technical Advisory groups (TAGs)
- DC3 Tool Expo

The contractor shall assist DC3 with pioneering D/MM forensic information (DFI) and remaining on the leading edge of computer technologies and techniques.

DFI Bulletins: The contractor shall screen, evaluate, and consolidate large quantities of information reports, intrusion investigations, law enforcement and CI case data from various sources that focus primarily on forensic information. The contractor shall publish two (2) DFI Bulletins per month.

The contractor shall review, analyze and prioritize all source information regarding criminal/terrorist/hacker threats that impact DoD computer systems. The contractor shall document and brief the identified threats, trends and issues to DC3.

The contractor shall develop requirements and methodologies to collect, analyze, and manage additional information supporting D/MM forensics. The contractor shall research and recommend further DCCI development in the D/MM forensic information for consideration.

The contractor shall assist in the development of a DFI portal to maintain templates, D/MM forensic database, steganography information, on-line training, forum discussion, validated file signature, and a legal library. The contractor shall research, compile, and update a digest of digital evidence case law/legislation and update, establish and maintain a Digital Evidence Library/CD. The contractor shall gather, research, and provide input for the expansion and enhancement of the DFI portal.

The contractor shall be responsible for setting up all DC3 Technical Advisory Group (TAG) meetings, and publishing minutes from each meeting.

The contractor shall be responsible for scheduling, coordinating, and vetting all vendor demonstrations.

C.6.5 TASK AREA 5 –OPERATIONS AND STAFF SUPPORT

The contractor shall communicate and articulate the role of DC3 relating to law enforcement/counterintelligence, computers and the D/MM forensics environment throughout the DoD.

The contractor shall assist DC3 in establishing and maintaining relationships and partnerships with forensic scientists, law enforcement, CI, academic institutions, private industries, legal professionals, international agencies, federal, state and local Governments. The contractor shall coordinate and collaborate on research and development initiatives within established networks.

The contractor shall assist in several DC3 outreach projects to include DC3 Cyber Files and Dispatch.

The contractor shall facilitate, participate and track tours, visitors, events, working groups and exchange programs**.**

The contractor shall develop and design DC3 D/MM forensic graphics and print media to include informational brochures, posters, logos, and displays.

C.6.5.1 TASK 5.1 – OUTREACH ACTIVITIES

The Contractor shall be responsible for the marketing, graphics and general outreach for DC3 to include:

- DC3 Dispatch, daily news email sent to internal and external recipients
- DC3 Cyber Files CD/DVD Containing Reports, Studies & Software
- DC3 speakers coordination
- Coordination of visitors and tours of DC3
- DC3 Information CDs/DVDs

The Contractor shall create and distribute the daily DISPATCH and maintain the SOP for the creation and distribution of the DISPATCH**.** The Contractor shall create and distribute DC3 Cyber Files and maintain the SOP for the creation and distribution of the Cyber Files**.**

The Contractor shall coordinate all press and media requests and activity as required.

The Contractor shall coordinate all media requests with appropriate Public Affairs office.

The Contractor shall coordinate all visitors and tours of DC3

The Contractor shall coordinate all DC3 briefings and speaker engagements.

The Contractor shall provide photography and graphics support for DC3 to include:

- Multimedia Production (animations)
- Physical Media Production (CDs/DVDs)
- DC3 logos, artwork, and DC3 branding
- Flyers and brochures

C.6.5.2 TASK 6.5.2 – DEFENSE INDUSTRIAL BASE CYBERSECURITY/INFORMATION ASSURANCE PROGRAM SUPPORT (DIB CS/IA)

The Contractor shall provide a subject matter expert (SME) to serve as a liaison to the DoD Chief Information Officer's DIB CS/IA Program Office to communicate DC3 equities on DoD

and national policy, to prepare DoD cyber policy recommendations, represent DC3 at DoD and interagency forums, and assist the DIB CS IA Program Office on a day-to-day basis.

The contractor shall provide expertise on DoD policy formulation, foreign cyber threats, DoD counterintelligence (CI), the intelligence community, and DoD sensitive activities.

The contractor shall interpret draft policy issuances and provide DC3 guidance on how they may affect the DC3 mission to support cyber threat information sharing, as well as its other mission areas in support of Law Enforcement (LE) and counterintelligence (CI) investigative support activities, (e.g., digital forensics and multi-media analysis for the Defense LE/CI Components, DoD cyber technical training, research, development, test, and evaluation, and cyber analytics.

The contractor shall represent DC3 and the DIB CS IA Program Office by performing outreach to industry when attending government and industry sponsored events, meetings and conferences.

The contractor shall perform other senior-level staff activities as required.

C.6.6 TASK AREA 6 – DCISE SUPPORT

The contractor must support Incident Reporting & Response as part of the DCISE service to participating DIB partners. The contractor must provide an interface with the DIB-CERT to receive and provide initial response to cyber security events reported by DIB partners. This response must include, but not be limited to:

- Within a timeline defined by current DCISE process, accept initial reporting of cyber security events from DIB partners
- Within a timeline defined by current DCISE process, produce initial report on severity of reported cyber security event
- Produce deep technical analysis and trending as required
- Perform data mining in support of customer requirements, to include basic tool development, database development, and other tasks as defined by best practice software development lifecycle management.
- Plan, coordinate and execute off-site quarterly technical exchanges with external entities.
- Manage the Capability Maturing Model Integration (CMMI) processes within DCISE
- Coordinating receipt of copies of malware (receiving copies of the actual offending software code and medium by which it was transmitted, which created the computer security event or incident), logs & affected media
- Develop and deliver Customer Response Forms (CRF) after receipt of Incident Collection Form (ICF) **[Section F, Deliverable 31].**
- Develop and deliver Technical Analysis Reports (TAR) after ICF receipt. **[Section F, Deliverable 32]**
- Develop and deliver Cyber Targeting Analysis Reports (CTAR) **[Section F, Deliverable 33].**
- Develop and deliver the daily Threat Information Product (TIP) Report [Section F, Deliverable 34] notifying DIB Partners of possible threats to their network infrastructure,

based on indicators derived solely from reports on intrusion activity in USG Stakeholder networks.

- As needed, develop and deliver CRF Supplements [Section F, Deliverable 35] to DIB Partners.
- Develop and deliver DIB Alerts [Section F, Deliverable 36] within 4 hour of a reported incident or security event to help DIB Partners identify potential compromised systems within their networks.
- Support development and delivery of annual updates to the DCISE Long Range Strategic Plan. **[Section F, Deliverable 37]**

C.6.7 TASK AREA 7 - DEFENSE CYBER CRIME CENTER ANALYTICAL GROUP (DC3-AG) SUPPORT

The contractor shall provide support for the DC3 – Analytical Group (AG) staff to mitigate propagation and impact on information stored on DIB networks as well as USG networks.

The contractor shall conduct cyber analysis in support of IA/CND analysis and investigation. The contractor shall provide a complete picture of the TTPs used by the attacker through D/MM forensics analysis of the media and other information provided by the DIB partner. In addition the contractor shall:

- Perform cyber analysis & report on malicious software involved
- Conduct cyber analysis on media
- Produce initial report on severity of reported cyber security event
- Produce deep technical analysis and trending as required
- Perform data mining in support of customer requirements, to include basic tool development, database development, and other tasks as defined by best practice software development lifecycle management.
- Coordinating receipt of copies of malware (receiving copies of the actual offending software code and medium by which it was transmitted, which created the computer security event or incident), logs & affected media

The contractor shall support the delivery of a Weekly Activity Report (WAR) to the DC3-AG Director containing associated contextual data from each member of DC3-AG reporting on products delivered, meetings attended, project updates, and issues faced by each team member. **[Section F, Deliverable 38].**

C.6.8 TASK AREA 8 -- PROVIDE DCFL FORENSIC EMERGENCY TECHNICAL SURGE SUPPORT (OPTIONAL CLIN 0003B)

The contractor shall also be available 24 hours a day, 7 days a week “on-call” Help Desk support. The contractor shall adhere to a robust industry standard for “on-call” support to include appropriate response times for solving problems based on mission criticality and priority as determined by the Government.

It is expected that there may be some unanticipated special cases that must be processed on an expedited basis. The contractor shall provide emergency technical support and advanced D/MM forensics technical support worldwide on short notice (e.g., two (2) workdays). It is anticipated that a typical team may include contractor personnel (forensic examiners) for a specified period of time to provide emergency support outlined in the following scenario:

Sample Scenario:

After a routine investigation OCONUS, an information technology asset was discovered that contains encrypted information that may put the US or its Allies in danger. After a surge requirement is determined by the Government, the contractor assembles a team to deploy OCONUS and provide emergency technical support within the scope of this task order. This support may include, but not be limited to, the following:

- D/MM forensics examiner support
- Case review (IT) and technical recommendations
- D/MM forensics lab analysis and reporting
- IT asset analysis and threat determination
- Vulnerability assessments and risk mitigation
- Information technology assessment and recommendations
- Oral presentations and the preparation of written findings and reports

End of Scenario

The unanticipated occurrences will be of a reasonable duration based on individual circumstances necessary to complete and then will end. The contractor shall not provide technical support outside the scope of this task order and shall only use the labor categories within the base contract. The use of higher skilled personnel to perform these duties shall be approved by the Government before incurrence. Deliverables for this task may include technical presentations, reports, and other technical products.

It is expected that there may be some unanticipated workload increases that necessitate 24 hours, 7 days/week support for specific tasks. The contractor shall provide 24X7 support for DCFL, NMO, DC3-AG, and DCISE tasks.

NOTE: The section numbers in this TO correspond to the section numbers in the Alliant Contract. Section D of the contractor's Alliant Contract is applicable to this TO and is hereby incorporated by reference. In addition, the following applies:

D.1 PRESERVATION, PACKAGING, PACKING, AND MARKING

The contractor shall deliver all electronic versions by email and CD-ROM as well as placing in the DC3 designated repository. Identified below are the required electronic formats, whose versions must be compatible with the latest, commonly available version on the market.

- Text MS Word
- Spreadsheets MS Excel
- Briefings MS PowerPoint
- Drawings MS Visio
- Schedules MS Project

NOTE: The section numbers in this TO correspond to the section numbers in the Alliant Contract. Section E of the contractor's Alliant Contract is applicable to this TO and is hereby incorporated by reference. In addition, the following applies:

E.2 PLACE OF INSPECTION AND ACCEPTANCE

Inspection and acceptance of all work performance, reports, and other deliverables under this TO will be performed by the client TPOC and the FEDSIM COR. Inspection and acceptance will occur at DC3 and FEDSIM.

E.3 SCOPE OF INSPECTION

All deliverables will be inspected for content, completeness, accuracy, and conformance to TO requirements by the FEDSIM COR. Inspection may include validation of information or software through the use of automated tools, testing, or inspections of the deliverables, as specified in the TO. The scope and nature of this inspection will be sufficiently comprehensive to ensure the completeness, quality, and adequacy of all deliverables.

The Government requires a period NTE 15 workdays after receipt of final deliverable items for inspection and acceptance or rejection.

E.4 BASIS OF ACCEPTANCE

The basis for acceptance shall be in compliance with the requirements set forth in the TO, the contractor's proposal and other terms and conditions of the contract. Deliverable items rejected shall be corrected in accordance with the applicable clauses.

For software development, the final acceptance of the software program will occur when all discrepancies, errors, or other deficiencies identified in writing by the Government have been resolved through documentation updates, program correction, or other mutually agreeable methods.

Reports, documents, and narrative-type deliverables will be accepted when all discrepancies, errors, or other deficiencies identified in writing by the Government have been corrected.

If the draft deliverable is adequate, the Government may accept the draft and provide comments for incorporation into the final version.

All of the Government's comments on deliverables must either be incorporated in the succeeding version of the deliverable, or the contractor must demonstrate to the Government's satisfaction why such comments should not be incorporated.

If the Government finds that a draft or final deliverable contains spelling errors, grammatical errors, or improper format, or otherwise does not conform to the requirements stated within this TO, the document may be immediately rejected without further review and returned to the contractor for correction and resubmission. If the contractor requires additional Government

guidance to produce an acceptable draft, the contractor shall arrange a meeting with the FEDSIM COR.

E.5 DRAFT DELIVERABLES

The Government will provide written acceptance, comments, and/or change requests, if any, within 15 workdays (unless specified otherwise in section F) from Government receipt of the draft deliverable. Upon receipt of the Government's comments, the contractor shall have ten workdays to incorporate the Government's comments and/or change requests and to resubmit the deliverable in its final form.

E.6 WRITTEN ACCEPTANCE/REJECTION BY THE GOVERNMENT

The CO/COR shall provide written notification of acceptance or rejection (Section J, Attachment K) of all final deliverables within 15 workdays (unless specified otherwise in section F). All notifications of rejection will be accompanied with an explanation of the specific deficiencies causing the rejection.

E.7 NON-CONFORMING PRODUCTS OR SERVICES

Non-conforming products or services will be rejected. Deficiencies will be corrected, by the contractor, within ten workdays of the rejection notice. If the deficiencies cannot be corrected within ten workdays, the contractor will immediately notify the FEDSIM COR of the reason for the delay and provide a proposed corrective action plan within ten workdays.

For FFP CLINs, if the contractor does not provide products or services that conform to the requirements of this TO, the Government will not pay the fixed price associated with the non-conforming products or services.

NOTE: The section numbers in this TO correspond to the section numbers in the Alliant Contract. Section F of the contractor's Alliant Contract is applicable to this TO and is hereby incorporated by reference. In addition, the following applies:

F.3 TASK ORDER PERIOD OF PERFORMANCE

The period of performance for this TO is a one-year base period and four, one-year options. They are as follows:

Base Year: January 27, 2012 - April 20, 2013
Option Year 1: April 21, 2013 - April 20, 2014
Option Year 2: April 21, 2014 - April 20, 2015
Option Year 3: April 21, 2015 - April 20, 2016
Option Year 4: April 21, 2016 – January 26, 2017

F.4 PLACE OF PERFORMANCE

The primary place of performance is DC3's facility in Anne Arundel County Maryland. There is also a small group of personnel providing support at the National Media Exploitation Center in the DC metropolitan area. The Government anticipates the addition of other DC3 facilities in Anne Arundel County Maryland during the period of performance of this Task Order. The Contractor shall also work at other Government and industry facilities as required.

The contractor will be required to provide support on during normal business hours, 5 days a week basis during daily hours of operations from 0730-1700. The contractor shall provide Help Desk support on a 12 hours per day, 5 days a week basis. "On-call" or extended support maybe required during emergency situations. Any alternate work schedules must be authorized by the Government.

Long distance travel (CONUS and OCONUS) is anticipated to be required in support of this effort.

F.5 DELIVERABLES

The following schedule of milestones will be used by the FEDSIM COR to monitor timely progress under this TO. The following abbreviations are used in this schedule:

NLT: No Later Than
TOA: Task Order Award
All references to Days: Government Workdays

Deliverables are due the next Government workday if the due date falls on a holiday or weekend.

The contractor shall submit the deliverables listed in the following table:

Deliverable Number (New)	Title	Brief Description	TO Reference	Original Deliverable Number (TO)	Generating Organization	Recipient	Planned Frequency
01	Kick-Off Meeting Agenda	The contractor shall provide a Project Kick-Off meeting agenda in accordance with the requirements in C.6.1.1.	C.6.1.1	01	PMO	TPOC; COR	NLT 6 days after TO award
02	Kick-Off Meeting Presentation	The contractor shall provide copies of the Project Kick-Off meeting presentation for all present at the Project Kick-Off meeting.	C.6.1.1	02	PMO	TPOC; COR	Kick-Off meeting
03	Draft PMP	The contractor shall provide a draft Program Management Plan (PMP) in accordance with the requirements in C.6.1.2.	C.6.1.2	03	PMO	TPOC; COR	Kick-Off meeting
04	PMP	The contractor shall provide a revised PMP incorporating Government comments from the Project Kick-Off meeting.	C.6.1.2	04	PMO	TPOC; COR	10 days after Kick-Off meeting
05	PMP Updates	Contractor works from a new version of the Program Management Plan (PMP) once approved by the Government (FEDSIM COR).	C.6.1.2 .1	05	PMO	TPOC;COR	Quarterly
06	Monthly Status Report (MSR)	The contractor Program Manager (PM) develops and provides an MSR to the DC3 TPOC and FEDSIM COR. The MSR includes information in accordance with the applicable requirements in C.6.1.3, including network performance metrics.	C.6.1.3	06	PMO	TPOC; COR	10th day of month

Deliverable Number (New)	Title	Brief Description	TO Reference	Original Deliverable Number (TO)	Generating Organization	Recipient	Planned Frequency
07	Trip Reports	Need is specified by the Government at the time of submission of request for travel. Trip information is in accordance with the requirements in C.6.1.3; Trip Reports are attached to the MSR for the period in which the travel occurred.	C.6.1.3	07	PMO	TPOC; COR	As needed; 10th day of month
08	Meeting Reports	Documents the results of meetings (with the Government); required information is reconciled with the official minutes if published (and Government lead is advised accordingly).	C.6.1.3	08	PMO	Relevant Government lead(s)	Within 72 hours
09	Problem Notification Reports (PNRs)	Contractor files a PNR to notify the COR of potential cost/schedule overruns/impacts, changing or incorrect assumptions on which tasks were based, etc..	C.6.1.3	09	PMO	COR	As needed
10	Weekly E-Mail Status Reports	Contractor provides weekly status (Word or Excel format) to Government (DC3) leads on status, adherence to project plans, if any, timelines, and problems, if any.	C.6.1.3	10	PMO	Relevant Government lead(s)	Fridays
11	Technical Status Meeting (TSM) Minutes	Contractor PM provides minutes of TSM, in accordance with C.6.1.4 requirements, to FEDSIM COR.	C.6.1.4	11	PMO	TPOC; COR	Within 5 calendar days
12	Transition In Plan	Contractor provides a plan to ensure minimum service disruption to vital Government business and no service degradation during and after transition.	C.6.1.7	25	PMO	TPOC; COR	Within 5 USG work days of award

Deliverable Number (New)	Title	Brief Description	TO Reference	Original Deliverable Number (TO)	Generating Organization	Recipient	Planned Frequency
13	Transition Out Plan	Contractor provides a plan to ensure a seamless transition from the incumbent to incoming contractor/government personnel at the expiration of the TO.	C.6.1.8	26	PMO	TPOC; COR	NLT ninety (90) calendar days prior to expiration of the TO
14	Monthly Resource Status Report	XP team will generate monthly status update of all projects (MOU/MOA, CRADA/EPA, Exercises, etc.) in preparation for status meeting with XP Director.	C.6.1.5 .1	12	XP	XP Director	10th day of month
15	Financial Initiative Tracking Analysis	CNCI Initiatives (Program Management Reviews (PMRs)) updated on a quarterly basis with values for funds received, obligated, and executed. Update to be provided to cognizant authorities, as needed.	C.6.1.5 .2	18	XP	XP Director and Cognizant government authorities	Quarterly
16	Executive Level Briefings	CNCI Initiatives (Program Management Reviews (PMR)) updated on a quarterly basis with values for funds received, obligated, and executed. Assist with presenting results of CNCI initiatives to the DC3 Director and other cognizant authorities, as needed.	C.6.1.5 .2	19	XP	DC3 Executive Director; Cognizant authorities	As needed

Deliverable Number (New)	Title	Brief Description	TO Reference	Original Deliverable Number (TO)	Generating Organization	Recipient	Planned Frequency
17	Trouble Call Status Reports (TCSRs)	Contains monthly metrics that report number of tickets opened/closed, average resolution time, types of trouble tickets, unusual patterns, unresolved tickets, and summary of hardware maintenance actions.	C.6.2	27 & 29	NMO	NMO Government Lead	10th day of month
19	Network Incident Report	Report on network faults, outages, and security incidents.	C.6.3.1	31	NMO	NMO Government Lead	As needed
20	Computer/Network Accounts Report	Report on number of network accounts created/deleted each quarter.	C.6.3.1	32	NMO	NMO Government Lead	Quarterly
21	Network Back-up Recovery Plan	Backup/recovery SOP listing all network equipment, backup timelines, and network recovery procedures.	C.6.3.1	34	NMO	NMO Government Lead	Initial document within 180 days of TOA; updated annually
22	Evidence discrepancy report	A report identifying any discrepancies in the receipt and handling of evidence.	C.6.3.14.1	54	DCFL	DCFL Director	As needed
23	D/MM Forensic Analysis Report (DFAR)	Forensic examination report compliant with all DC3 procedures.	C.6.3.14.1	55	DCFL	DCFL Section Chiefs	Ongoing
24	DCFL Section Objectives Document	Document objectives and core processes for each DCFL Section.	C.6.3.14.2	60	DCFL	DCFL Director; DCFL Section Chiefs	Initial document within 180 days of TOA; updated annually
25	DCFL Certification and Training Status Report	Report on certification and training status for personnel in DCFL.	C.6.3.14.3	64	DCFL	DCFL Director	Quarterly
26	DCCI Request Status Report	Quarterly status report on all requests of DCCI.	C.6.4.1	70	DCCI	DCCI Director	Quarterly

Deliverable Number (New)	Title	Brief Description	TO Reference	Original Deliverable Number (TO)	Generating Organization	Recipient	Planned Frequency
27	Analysis Report	Provide written analysis of all requests outside scope or problematic to DC3 regulations, as needed. Analysis will explain why Form 10 is not valid to pursue and present possible remedies to the request to satisfy the needs of the organization.	C.6.4.1	71	DCCI	DCCI Director	As needed
28	Requirements Documentation, Design Documents, User Manuals	Project plans and requirement documentation are defined by the DCCI software development guide. Procedures are followed for all medium to large development projects.	C.6.4.1	72	DCCI	DCCI Director	Ongoing
29	Weekly Activity Report	The Weekly Activity Report informs the government of previous week's activities performed by the contractors within DCCI.	C.6.4.1	74	DCCI	DCCI Director	Fridays
Reserved							
31	Customer Response Form (CRF)	The CRF provides cyber situational awareness to the DIB, USG, and Critical Infrastructure /Key Resource (CI/KR) community on an event or incident reported by a DIB or CI/KR Partner through an Incident Collection Form (ICF). The CRF summarizes the event using incident details and malware analysis.	C.6.6	94	DCISE	Defense Industrial Base POCs	Within 72 hours after receipt of Incident Collection Form (ICF)

Deliverable Number (New)	Title	Brief Description	TO Reference	Original Deliverable Number (TO)	Generating Organization	Recipient	Planned Frequency
32	Threat Activity Report (TAR)	The TAR is an in-depth analytic product that correlates technical activities and indicators from across the DIB, with activity identified in the broader Information Assurance community. TARs offer a larger set of indicators of related reporting and provide DIB Partners greater context into the network intrusion/events.	C.6.6	95	DCISE	Defense Industrial Base POCs	Within 10 working days after assignment
33	Cyber Targeting Analysis Report (CTAR)	The CTAR is a strategic-level, INFOSEC analytic report that provides DIB Partners with insight into technology targeting. CTAR analysis is derived from ICFs, CRFs, TARs, and other INFOSEC and Intelligence Community reporting.	C.6.6	96	DCISE	Defense Industrial Base POCs	Within 30 working days of activity recognition
34	Threat Information Product (TIP) Report	The TIP is a daily report that notifies DIB Partners of possible threats to their network infrastructure. TIPs contain cyber indicators derived solely from reports on intrusion activity experienced in USG Stakeholder networks.	C.6.6	N/A	DCISE	Defense Industrial Base POCs	Daily
35	Customer Response Form (CRF) Supplement	See CRF (Deliverable 31) Description above.	C.6.6	N/A	DCISE	Defense Industrial Base POCs	As Needed

Deliverable Number (New)	Title	Brief Description	TO Reference	Original Deliverable Number (TO)	Generating Organization	Recipient	Planned Frequency
36	DIB Alert	The DIB Alert is a time-sensitive product released to the DIB Partner community. The product contains indicators that help partners and community stakeholders identify potential compromised systems within their respective networks.	C.6.6	N/A	DCISE	Defense Industrial Base POCs	Within 4 hours of a reported incident or security event derived from internal or external sources
37	DCISE Long Range Strategic Plan	The DCISE Long Range Strategic Plan includes the strategy and initiatives necessary to achieve the goals of the organization. The plan is updated on an annual basis and the deliverable is a written document.	C.6.6	N/A	DCISE	DCISE Director	Annually (May)
38	Weekly Activity Report (WAR)	Weekly Activity Report (WAR) contains series of bullets with associated contextual data from each member of DC3-AG that report on products delivered, meetings attended, project updates, and issues faced by each team member.	C.6.7	N/A	DC3-AG	DC3 –AG Director	Fridays

F.6 PUBLIC-RELEASE OF CONTRACT DOCUMENTS REQUIREMENT

The contractor agrees to submit, within ten business (10) days from the date of the Contracting Officer's execution of the initial TO, or any modification to the TO (exclusive of Saturdays, Sundays, and Federal holidays), a portable document format (PDF) file of the fully executed document with all proposed necessary redactions, including redactions of any trade secrets or any commercial or financial information that it believes to be privileged or confidential business information, for the purpose of public disclosure at the sole discretion of GSA. The contractor agrees to provide a detailed written statement specifying the basis for each of its proposed redactions, including the applicable exemption under the Freedom of Information Act (FOIA), 5 U.S.C. § 552, and, in the case of FOIA Exemption 4, 5 U.S.C. § 552(b)(4), shall demonstrate

why the information is considered to be a trade secret or commercial or financial information that is privileged or confidential. Information provided by the contractor in response to the contract requirement may itself be subject to disclosure under the FOIA. Submission of the proposed redactions constitutes concurrence of release under FOIA.

GSA will carefully consider all of the contractor's proposed redactions and associated grounds for nondisclosure prior to making a final determination as to what information in such executed documents may be properly withheld.

F.7 PLACE(S) OF DELIVERY

Unclassified deliverables and correspondence shall be delivered to the GSA Contracting Officer (CO) or Contracting Officer's Representative (COR) at the address below:

GSA FAS AAS FEDSIM
ATTN: Keith A. Parks, COR
1800 F St NW
Washington DC 20405
Phone: 703-605-3648
FAX: 703-605-9894
Email: keith.parks@gsa.gov

Copies of all deliverables shall also be delivered to the DC3 TPOC at the address below:

Mr. William Jimenez
Deputy Director (Chief Operating Officer)
Defense Cyber Crime Center (DC3)
Office: 410-981-1188
Fax: 410-850-8906
BBerry: (b) (6)
Email: william.jimenez@dc3.mil
Phone: (410) 981-0117
Fax (410) 981-0183

F.8 NOTICE REGARDING LATE DELIVERY/PROBLEM NOTIFICATION REPORT (PNR)

The contractor shall notify the FEDSIM COR via a Problem Notification Report (PNR) (Section J, Attachment J) as soon as it becomes apparent to the contractor that a scheduled delivery will be late. The contractor shall include in the PNR the rationale for late delivery, the expected date for the delivery, and the project impact of the late delivery. The FEDSIM COR will review the new schedule and provide guidance to the contractor. Such notification in no way limits any Government contractual rights or remedies including, but not limited to, termination.

NOTE: The section numbers in this TO correspond to the section numbers in the Alliant Contract. Section G of the contractor's Alliant Contract is applicable to this TO and is hereby incorporated by reference. In addition, the following applies:

G.3.5 CONTRACTING OFFICER'S REPRESENTATIVE

The CO will appoint a COR in writing for each TO. The COR will receive, for the Government, all work called for by the TO and will represent the CO in the technical phases of the work. The COR will provide no supervisory or instructional assistance to contractor personnel.

The COR is not authorized to change any of the terms and conditions, scope, schedule, and price of the Contract or the TO. Changes in the scope of work will be made only by the CO by properly executed modifications to the Contract or the TO.

G.9.6 INVOICE SUBMISSION

The contractor shall submit Requests for Payments in accordance with the format contained in GSAM 552.232-25, PROMPT PAYMENT (NOV 2009), to be considered proper for payment. In addition, the data elements indicated below shall be included on each invoice.

Task Order Number: *(from GSA Form 300, Block 2)*
Paying Number: *(ACT/DAC NO.) (From GSA Form 300, Block 4)*
FEDSIM Project Number: (Fill in project number)
Project Title: DC3 Cyber Crime Support

The contractor shall certify with a signed and dated statement that the invoice is correct and proper for payment.

The contractor shall provide invoice backup data in accordance with the contract type, including detail such as labor categories, rates, and quantities of labor hours per labor category.

The contractor shall submit invoices as follows:

The contractor shall utilize FEDSIM's electronic Tracking and Ordering System (TOS) to submit invoices. The contractor shall submit invoices electronically by logging onto the following link (requires Internet Explorer to access the link):

https://portal.fas.gsa.gov

Select *Vendor Support*, log in using your assigned ID and password, then click on *Create Invoice*. The TOS Help Desk should be contacted for support at 877-472-4877 (toll free). By utilizing this method, no paper copy of the invoice shall be submitted to GSA FEDSIM or the GSA Finance Center. However, the FEDSIM COR may require the contractor to submit a written "hardcopy" invoice with the client's certification prior to invoice payment.

G.9.6.1 INVOICE REQUIREMENTS

The contractor may invoice the fixed fee on a monthly basis. The monthly fixed fee invoiced shall be proportionate to the amount of labor expended for the month invoiced.

The contractor shall submit simultaneous copies of a draft or advance copies of an invoice to both GSA and the client POC.

If the TO has different contract types, each should be addressed separately in the invoice submission.

The final invoice is desired to be submitted within six months of project completion.

G.9.6.1.1 COST-PLUS-FIXED-FEE (CPFF) CLINs (for LABOR)

The contractor may invoice monthly on the basis of cost incurred for the CPFF CLINs. The invoice shall include the period of performance covered by the invoice and the CLIN number and title. All hours and costs shall be reported by CLIN element (as shown in Section B) and contractor employee and shall be provided for the current billing month and in total from project inception to date. The contractor shall provide the invoice data in spreadsheet form with the following detailed information. The listing shall include separate columns and totals for the current invoice period and the project to date.

- Employee name (current and past employees)
- Employee company labor category
- Employee Alliant labor category
- Monthly and total cumulative hours worked
- Billing rate (as proposed in the cost proposal)
- Corresponding Alliant Task rate
- Fixed fee
- Cost incurred not billed

All cost presentations provided by the contractor shall also include Overhead charges, and General and Administrative charges.

G.9.6.1.2 FIRM-FIXED-PRICE (FFP) CLINS

The contractor may invoice as stated in Section B for the FFP CLINs. The invoice shall include the period of performance/deliverable or progress payment period covered by the invoice and the CLIN number and title. All costs shall be reported by CLIN element (as shown in Section B) and shall be provided for the current invoice and in total from project inception to date. The contractor shall provide the invoice data in spreadsheet form with the following detailed information. The listing shall include separate columns and totals for the current invoice period and the project to date.

- FFP (period of performance/deliverable or progress payment period – as stated in Section B)

G.9.6.1.3 OTHER DIRECT COSTS (ODCs)

The contractor may invoice monthly on the basis of cost incurred for the ODC CLIN. The invoice shall include the period of performance covered by the invoice and the CLIN number and title and Interagency Agreement (IA) number. In addition, the contractor shall provide the following detailed information for each invoice submitted, as applicable. Spreadsheet submissions are required.

- Tools and/or ODCs purchased
- Consent to Purchase number or identifier
- Date accepted by the Government
- Associated CLIN
- Project–to-date totals by CLIN
- Cost incurred not billed
- Remaining balance of the CLIN

All cost presentations provided by the contractor shall also include Overhead Charges, General and Administrative Charges, and Fee.

G.9.6.1.4 LONG DISTANCE TRAVEL

The contractor may invoice monthly on the basis of cost incurred for cost of travel comparable with the Joint Travel Regulation (JTR)/Federal Travel Regulation (FTR). Long distance travel is defined as travel over 50 miles. The invoice shall include the period of performance covered by the invoice, the CLIN number and title, and the IA number. Separate worksheets, in MS Excel format, shall be submitted for travel.

CLIN/Task Total Travel: This invoice information shall identify all cumulative travel costs billed by CLIN/Task. The current invoice period's travel details shall include separate columns and totals and include the following:

- Travel Authorization Request number or identifier, approver name, and approval date
- Current invoice period
- Names of persons traveling
- Number of travel days
- Dates of travel
- Number of days per diem charged
- Per diem rate used
- Total per diem charged
- Transportation costs
- Total charges
- Explanation of variances exceeding 10% of the approved versus actual costs
- Indirect Handling Rate

All cost presentations provided by the contractor shall also include Overhead charges and General and Administrative charges.

G.10 CONTRACT ADMINISTRATION

Contracting Officer:

GSA FAS AAS FEDSIM
ATTN: Denise VonDibert, CO
1800 F St NW
Washington, DC 20405
Telephone: (703) 605-3633
Fax: (703) 605-0000
Email: denise.vondibert@gsa.gov

Contracting Officer's Representative:

GSA FAS AAS FEDSIM
ATTN: Keith Parks, COR
1800 F St NW
Washington, DC 20405
Phone: 703-605-3648
FAX: 703-605-9894
Email: keith.parks@gsa.gov

Technical Point of Contact:

Mr. William Jimenez
Email: william.jimenez@dc3.mil

NOTE: The section numbers in this TO correspond to the section numbers in the Alliant Contract. Section H of the contractor's Alliant Contract is applicable to this TO and is hereby incorporated by reference. In addition, the following applies:

H.2 KEY PERSONNEL

The following are the minimum personnel who shall be designated as "Key." The contractor shall propose appropriate labor categories for these positions. The Government does not intend to dictate the composition of the ideal team to perform this TO. Therefore, the Government encourages and will evaluate additional Key Personnel as proposed by the offeror.

- Program Manager
- DCFL Lead D/MM Forensic Technician
- DCFL Lead D/MM Forensic Examiner
- NMO Senior Systems/Network Engineer
- Senior Software Engineer
- Lead Cyber Intelligence Analyst
- NMO Information Assurance Specialist
- DCISE Task Lead

The Government desires that Key Personnel be assigned for the duration of the TO.

H.2.3 PROGRAM MANAGER

It is desirable that the Program Manager (PM) has the following qualifications:

- Demonstrated strong managerial experience in providing technical advice, organizing, planning, directing, and managing contractor staff.
- Successfully manage complex projects/operations of a nature similar in size and scope as referenced under this Task Order.
- Experience with the current cyber crime environments, labs or environments similar to DC3.
- Successfully manage and supervise employees (50 or more) of various labor categories and skills in projects similar in size and scope as referenced under this Task Order.
- Understanding and experience with financial and performance monitoring, e.g., performance metrics.
- Identifying user requirements; translating the requirements into project plans and milestones; directing and implementing plans; and presenting formal project status/plan briefings to the Government managers.

H.2.4 OTHER KEY PERSONNEL

H.2.4.1 DCFL LEAD D/MM FORENSIC TECHNICIAN

It is desirable that the DCFL Lead D/MM Forensic Technician has the following qualifications:

- Experience in handling evidence and performing forensically sound duplication of original evidence.
- Advanced experience in data imaging and extraction and be capable of conducting peer reviews of cases completed by other examiners.
- Knowledge of DoD SCIF, lab, and network security policies protocols.
- Extensive experience with all versions of Microsoft windows, Apple and Linux operating systems.
- Experience utilizing imaging software such as FTK, Safeback, EnCase or similar.
- Experience supervising and managing a team of 3 or more personnel.

H.2.4.2 DCFL LEAD D/MM FORENSIC EXAMINER

It is desirable that the DCFL Lead D/MM Forensic Examiner demonstrate the following qualifications:

- Working knowledge of D/MM forensics and techniques.
- Strong technical skills in D/MM forensics and examining computer media.
- Experience in conducting substantive analysis and examination of computers and media generated by computers.
- Extensive experience with all versions of Microsoft windows, Apple and Linux operating systems.
- Knowledge of DoD SCIF, lab, and network security policies protocols.
- Ability to properly and accurately document examination findings.
- Experience supervising and managing a team of 3 or more personnel.

H.2.4.3 NMO SENIOR SYSTEMS/NETWORK ENGINEER

It is desirable that the NMO Senior Systems/Network Engineer demonstrate the following qualifications:

- Up to date training and certification such as Global Information Assurance Certification (GSEC), Microsoft Certified Systems Engineer (MCSE), Computing Technology Industry Association (CompTIA A+), and CISCO Certified Senior Systems Engineer.
- Cisco Certified Network Associate (CCNA) or equivalent.
- Red Hat Certified Engineer (RHCE) or equivalent.
- Strong technical skills and experience in managing, monitoring, and controlling networks and systems similar in size, complexity, and scope to the DC3 environment.
- Knowledge of IT infrastructures similar to the DC3 environment.
- Experience with system and network security implementation and management.

- Knowledgeable in DC3, AFOSI, USAF and the Department of Defense (DoD) Information Technology, policy, procedures, and technical communication requirements to include the following:
    - AFI 33-138 Enterprise Networks Operations Notification and Tracking
    - AFI 33-202 Network and Computer Security
    - AFI 33-114 Communications and Information Software Management
    - DoD Directive 8570. 1-M Information Assurance Training, Certification, and Workforce Management.
- Administrating and configuring PC systems, trouble-shooting, and resolving PC systems, network servers, and networks system in the Microsoft and Linux-based network system environments.
- Monitoring network status; recommending system/network change requests.

H.2.4.4 SENIOR SOFTWARE ENGINEER

It is desirable that the Senior Software Engineer demonstrate the following qualifications:

- Experience with policy and procedures regarding technology development and testing in the DoD.
- Knowledge of D/MM forensic technology and capable of analyzing and making recommendations to DCCI leadership regarding forensic research, development, testing and evaluation.
- Knowledge of the Department of Defense and Air Force policies.
- Experience with common programming techniques and high level programming languages to include C++, PERL, JAVA and other scripting languages.
- Ability to develop technical solutions to complex problems.
- Experience in conducting testing and evaluation on software, hardware and processes.

H.2.4.5 LEAD CYBER INTELLIGENCE ANALYST

It is desirable that the Lead Cyber Intelligence Analyst demonstrate the following qualifications:

- Experience developing requirements and methodologies to collect, analyze, manage and present intelligence in support of D/MM forensics.
- Knowledge of principals, concepts, and methodologies of intelligence analysis.
- Knowledge of the U.S. Intelligence Community and related Government, industrial, and academic communities to include knowledge of U.S. intelligence collection systems, capabilities and limitations and Intelligence Community policy.
- Experience assimilating large amounts of information, logically analyzing it and ability to write succinctly about the analysis.
- Experience with Information Assurance and Signals Intelligence (SIGINT).
- Knowledge and experience with computer and network operating systems.

H.2.4.6 NMO INFORMATION ASSURANCE SPECIALIST

It is desirable that the NMO Information Assurance Specialist demonstrate the following qualifications:

- Meets all Department of Defense educational and certification requirements.
- Knowledge and experience commensurate with CISSP, CCNA, CCSA and Network+ certifications (certification preferred).
- Extensive experience with security, system auditing and hacking tools.
- Strong working knowledge of VPN and encryption technologies.
- Familiarity with mobile code, malicious code and Anti-Virus software.
- Knowledge of wireless protocols and wireless security
- Experience analyzing network traffic to identify anomalies in a high volume enterprise environment.
- Experience hardening operating systems, including but not limited to: Windows NT/2000, Linux, Solaris, and HP-UX.
- Experience implementing Intrusion Detection Systems (network and host based) and developing custom signatures to try to stay alert of current security trends.
- Experience with Physical Security methods.
- Ability to document processes and procedures clearly and accurately.
- Ability to stay abreast of internal and external security best practices.

H.2.4.7 DCISE TASK LEAD

It is desirable that the DCISE Task Lead demonstrate the following qualifications:

- Extensive background in Management Information Systems / Computer Science.
- Professional Project Management (PMP) certification.
- Experience performing strategic planning with demonstrated experience
- Strong understanding of computer network defense, cyber security, and information assurance
- Strong Project Management skills with demonstrated experience.
- Excellent working knowledge of Microsoft Office (Word, Excel, PowerPoint, Visio).
- Working knowledge of Microsoft Project.
- Excellent oral and written communication skills.
- Must be process oriented and have strong organizational skills.
- Ability to work with a sense of urgency and attention to detail.
- Good interpersonal skills.

H.2.5 KEY PERSONNEL SUBSTITUTION

The contractor shall not replace any personnel designated as Key Personnel without the written concurrence of the CO. Prior to utilizing other than personnel specified in proposals in response to a TOR, the contractor shall notify the Government CO and the COR of the existing TO. This notification shall be no later than ten calendar days in advance of any proposed substitution and shall include justification (including resume(s) and labor category of proposed substitution(s)) in sufficient detail to permit evaluation of the impact on TO performance.

Substitute personnel qualifications shall be equal to, or greater than, those of the personnel being substituted. If the Government CO and the COR determine that the proposed substitute personnel is unacceptable, or that the reduction of effort would be so substantial as to impair the successful performance of the work under the TO, the contractor may be subject to default action as prescribed by FAR 52.249-6, Termination (Cost Reimbursement) or FAR 52.249-8, Default (Fixed-Price Supply and Service).

H.5 GOVERNMENT-FURNISHED PROPERTY (GFP)

The Government will provide on-site office facilities and office equipment for Contractor personnel at DC3 locations.

H.5.2 GOVERNMENT-FURNISHED INFORMATION (GFI)

The Government will provide the following information on the date of award:

- DCFL Personnel Handbook
- DCFL SOP
- DCCI Personnel Handbook

H.7 SECURITY CONSIDERATIONS

H.7.1 SECURITY REQUIREMENTS

This is a Department of Defense (DoD) work effort involving access to and the safeguarding of classified information/material. The security policies, procedures and requirements stipulated in the National Industrial Security Program (NISP); National Industrial Security Program Operating Manual (NISPOM) and any supplements thereto are applicable; to include, applicable Federal Acquisitions Regulations (FAR) and Defense Federal Acquisition Regulations (DFARS). The Contractor shall also comply with DoD 5200.1-R and Air Force security regulations and guidance.

The contractor shall meet the Government personnel security, information security and physical security requirements at Contractor sites, Government CONUS and OCONUS facilities. Specifically, the Contractor shall have a current Top Secret facility clearance. Additionally, all contractor personnel working in a SCIF are required to have the following:

a. Have undergone an SSBI or SSBI-PR within the last five (5) years that was favorably adjudicated;
b. Have no break, greater than 24 months, in military service, federal civilian employment or access to classified information under the Industrial Security Program;
c. Possess a current Top Secret security determination;
d. Possess a Sensitive Compartmented Information determination reflected in JPAS or Scattered Castles.

In order to report to a Sensitive Compartmented Information Facility (SCIF) for the first day of employment, contractor personnel must possess a current TS clearance with a Sensitive Compartmented Information (SCI) determination reflected in JPAS or Scattered Castles and be formally nominated by their company's security office to be indoctrinated into SCI programs.

If any contracted personnel are *unable to obtain* a Top Secret clearance with access to SCI within 180 calendar days of employment by the contractor in support of this contract and for employment in a SCIF, the contractor shall:

a. Notify the government; and,
b. Terminate billing for the employee against the contract if required by the Government.

If any contracted personnel employed by the contractor in support of this contract, *fail to maintain* the required security clearance or access, or are involved in an incident which could jeopardize their access to classified material, the contractor shall:

a. Notify the government of this discrepancy; and,
b. Remove the employee from the DC3 site; and,
c. Terminate billing for the employee against the contract.

H.7.2 SECURITY CLEARANCES

All contractor personnel supporting this Task Order require a security clearances as stated below, depending on what area the contractor employee is assigned prior to award. In all cases, the Contractor shall forward employee investigation information to the COR and DC3 TPOC before assignment of these individuals on Task Order and shall ensure a visit request with that investigation information is provided yearly. Contract employees to perform work assignments within the DC3 that do work in the SCIF are required to obtain at least an interim secret clearance with the ability to process and maintain a final secret.

The contractor shall provide personnel with the following security classifications by specific discipline outlined below:

1. Program Manager (Key): TS-SCI
2. DCFL Lead D/MM Forensic Examiners (Key): TS-SCI,
3. D/MM Forensic Examiners: 60% are required to have TS-SCI, 40% are required to have active Secret
4. DCFL Lead D/MM Forensic Technician (Key): TS-SCI,
5. D/MM Forensic Examiners: 60% are required to have TS-SCI, 40% are required to have active Secret
6. Evidence Custodians: 60% are required to have TS-SCI, 40% are required to have active Secret
7. NMO Senior Systems/Network Engineer (Key): TS-SCI
8. Senior Software Engineer (DCCI) (Key): TS-SCI
9. DC3-AG Personnel: 100% are required to have TS-SCI
10. Security Personnel: 100% are required to have TS-SCI

11. Administrative Personnel: 100% are required to have a Secret
12. DCISE Personnel: 75% are required to have TS-SCI, and 25% active Secret
13. NMO Personnel: 50% are required to have TS-SCI, and 50% active Secret
14. DCCI Personnel: 75% are required to have TS-SCI, and 25% active Secret
15. FM and XP Personnel: 50% are required to have TS-SCI and 50% active Secret

All Contractor personnel will be required to obtain and maintain TS-SCI access as required by DC3 Mission growth.

The Government retains the right to request removal of Contractor personnel, regardless of prior clearance or adjudication status, whose actions while assigned, to this Task Order conflict with the interests of the Government. The reason for removal will be fully documented in writing by the FEDSIM COR in coordination with the DC3 TPOC.

All contractor personnel possessing a security clearance and working in a Sensitive Compartmented Information Facility (SCIF) environment according to AF standards shall be subject to random Counterintelligence Security Polygraphs (CISP) and urine analysis.

A DD254 (Section J, Attachment B) will be provided at time of award.

H.7.3 AIR FORCE PRIVACY AND SECURITY REQUIREMENTS

This is a Department of Defense (DoD) work effort involving access to and/or the safeguarding of classified information/material. The security policies, procedures and requirements stipulated in the National Industrial Security Program (NISP) and National Industrial Security Program Operating Manual (NISPOM) and any supplements thereto are applicable. To include, applicable Federal Acquisitions Regulations (FAR), Defense Federal Acquisition Regulations (DFARS) and Air Force Federal Acquisition Regulations (AFFARS) security provisions and/or clauses. AFFARS Clause 5352-204-9000, Notification of Security Activity and Visitor Group Security Agreement (VGSA) is applicable to this effort whenever task order performance occurs on an Air Force installation or within an Air Force controlled facility or activity.

This work effort involves the contractor having access to and/or safeguarding of classified information/material and shall require Top Secret clearances with SCI eligibility and other security accesses (Critical Nuclear Weapons Design Information (CNWDI), Restricted Data, Formerly Restricted Data, NATO, SAP, SAR, COMSEC) identified by the DC3 for task order performance. Other work performed under this task order may require lower clearance levels appropriate for task order performance. Contractors having access to and/or safeguarding classified information/material shall require the appropriate security clearance. The security policies, procedures and requirements stipulated in the NISP; NISPOM and supplements thereto are applicable, to include the following security requirements and/or guidance whenever task order performance will occur on a DoD installation or within a DoD controlled facility or activity:

a. The contractor shall possess or acquire a facility clearance equal to the highest classification stated in the above paragraph in accordance with the NISPOM for task order performance.

b. Disclosure of Information: The contractor shall not release to anyone outside the contractor's organization any classified information, regardless of medium (e.g., film, tape, document, etc.), pertaining to any part of this task order or any program related to this task order, unless: (1) The Contracting Officer has given prior written approval; or (2) The information is otherwise in the public domain before the date of release. Request for approval shall identify the specific information to be released, the medium to be used, and the purpose for the release. The contractor shall submit its request to the Contracting Officer at least 45 days before the proposed date for the release. The contractor agrees to include a similar requirement in each subcontract under this task order. Sub contractors shall submit request for authorization to release through the prime contractor to the Contracting Officer.

c. The contractor's procedures for protecting against unauthorized disclosure of information shall not require Department of Defense employees or members of the Armed Forces to relinquish control of their work product, whether classified or not, to the contractor.

d. Prior to beginning operations involving classified information at the Government facility, the contractor must possess, or acquire prior to award of a contract, a facility clearance equal to the highest classification stated on the Contract Security Classification Specification 9, DD Form 254, attached to this solicitation, the contractor shall enter into a security agreement (or understanding) with the local Government security office. This will ensure contractors follow local security procedures while performing at the Government facility. As a minimum, the agreement shall identify the security actions that will be performed: (a) By the Government facility for the contractor, such as providing storage and classified reproduction facilities, guard services, security forms, security reviews under DoD 5220.22-M, classified mail services, security badges, visitor control, and investigating security incidents; and (b) Jointly by the contractor and the installation, such as packaging and addressing classified transmittals, security checks, internal security controls, and implementing emergency procedures to protect classified information.

e. Pursuant to Section 808 of Pub. L. 102-190 (DFAS 204, Subpart 204.402(2)), DoD employees or members of the Armed Forces who are assigned to or visiting a contractor facility and are engaged in oversight of an acquisition program will retain control of their work product. Classified work products of DoD employees or members of the Armed Forces shall be handled in accordance with DoD 5220.22-M. Contractor procedures for protecting against unauthorized disclosure of information shall not require DoD employees or members of the Armed Forces to relinquish control of their work products, whether classified or not, to a contractor.

f. If a visit to a contractor facility will require access to classified information, the visitors must give the contractor advance written notice.

g. When task order performance will involve classified information, the contracting officer shall ensure that the DD Form 254, Contract Security Classification Specification, includes the complete mailing address of the Information Security Program Manager (ISPM) and the responsible Major Command (MAJCOM) security forces. Promptly after task order award,

the contracting officer shall provide a copy of the DD Form 254 to each addressee on the DD Form 254.

h. Work on this project may require that personnel have access to Privacy and other sensitive information. Personnel shall adhere to the Privacy Act, Title 5 of the United States code, section 552a and applicable Client Agency rules and regulations.

i. Contractor personnel shall not divulge or release privacy data or information developed or obtained in the performance of this task order, until made public or specifically authorized by the Government. The contractor shall not use, disclose, or reproduce third party companies' proprietary data, other that as authorized and required in performance of this task order. Personnel working on this project will be required to sign a non-disclosure agreement **(Section J, Attachment F)** immediately upon their start on the project, electronic signatures are also acceptable. The contractor's procedures for protecting against unauthorized disclosure of information shall not require Department of Defense employees or members of Armed Forces to relinquish control of their work product, whether classified or not, to the contractor.

j. All Research, Development, Test and Evaluation Projects accomplished by contractor personnel in support of this Task Order become the Intellectual Property of DC3 and the US Government.

Where classified information/data is involved, the Contractor shall comply with the "National Industrial Security Program Operating Manual (NISPOM)" and the DD Form 254 (Contract Security Classification Specification) that is included per DD254 in Section J, Attachment 2 (Ref FAR 52.204-2).

The Contractor will be required to comply with all security requirements ~~i~~n accordance with DoD 5200.2-R, Personal Security Program, Contractor personnel shall have as a minimum a favorable National Agency Check (NAC) completed before being permitted access to any Government automated information technology system.

H.7.4 FOREIGN CONTRACTORS

In accordance with the DD Form 254, foreign firms or foreign-owned firms will not be permitted to participate as prime contractors, unless they have been approved by Defense Security Service (DSS) under the Foreign Ownership, Control, or Influence (FOCI) process to receive a facility security clearance. In accordance with the National Industrial Security Program Operating Manual (NISPOM) and FOCI, security measures must be established to mitigate the foreign ownership in order to receive a facility security clearance. A foreign-owned company may also be cleared under a Special Security Agreement (SSA). If an SSA-cleared company requires access to prescribed information (e.g. Top Secret - Sensitive Compartmented Information (TS-SCI)), a National Interest Determination (NID) will be processed and approved to declare that release of information would not harm the national security interests of the United States.

H.9 ORGANIZATIONAL CONFLICT OF INTEREST AND NON-DISCLOSURE REQUIREMENTS

H.9.1 ORGANIZATIONAL CONFLICT OF INTEREST

If the contractor is currently providing support or anticipates providing support to DC3 that creates or represents an actual or potential organizational conflict of interest (OCI), the contractor shall immediately disclose this actual or potential OCI in accordance with FAR Subpart 9.5. The contractor is also required to complete and sign an Organizational Conflict of Interest Statement in which the contractor (and any Subcontractors, consultants or teaming partners) agrees to disclose information concerning the actual or potential conflict with any proposal for any solicitation relating to any work in the TO. All actual or potential OCI situations shall be identified and addressed in accordance with FAR Subpart 9.5.

H.9.2 NON DISCLOSURE REQUIREMENTS

If this TO requires the contractor to act on behalf of, or provide advice with respect to any phase of an agency procurement, as defined in FAR 3.104-4, then the contractor shall ensure that all its personnel (to include subcontractors, teaming partners, and consultants) who will be personally and substantially involved in the performance of the TO:

- Execute sign (electronic signatures are also acceptable and submit an Employee/Contractor Non-Disclosure Agreement (NDA) Form (Section J, Attachment F)) prior to the commencement of any work on the TO, and
- Are instructed in the FAR 3.104 requirements for disclosure, protection, and marking of contractor bid or proposal information, or source selection information.

All proposed replacement contractor personnel also must submit an NDA and be instructed in the requirements of FAR 3.104. Any information provided by contractors in the performance of this TO or obtained by the Government is only to be used in the performance of the TO. The contractor shall put in place appropriate procedures for the protection of such information and shall be liable to the Government for any misuse or unauthorized disclosure of such information by its personnel, as defined above.

H.18 PURCHASING SYSTEMS

The objective of a contractor purchasing system assessment is to evaluate the efficiency and effectiveness with which the contractor spends Government funds and complies with Government policy with subcontracting.

Prior to the award of a TO the CO shall verify the validity of the contractor's purchasing system. Thereafter, the contractor is required to certify to the CO no later than 30 calendar days prior to the exercise of any options the validity of their purchasing system. Additionally, if reviews are conducted of the purchasing system after the exercise of the option, the contractor shall provide the results of the review to the CO within 10 workdays from the date the results are known to the contractor.

H.23 TRAVEL

H.23.1 TRAVEL REGULATIONS

Contractor costs for travel will be reimbursed at the limits set in the following regulations (see FAR 31.205-46):

(1) Federal Travel Regulations (FTR) - prescribed by the GSA, for travel in the contiguous U.S.

(2) Joint Travel Regulations (JTR), Volume 2, Department of Defense (DoD) Civilian Personnel, Appendix A - prescribed by the DoD, for travel in Alaska, Hawaii, and outlying areas of the U.S.

(3) Department of State Standardized Regulations (DSSR) (Government Civilians, Foreign Areas), Section 925, "Maximum Travel Per Diem Allowances for Foreign Areas" - prescribed by the Department of State, for travel in areas not covered in the FTR or JTR.

H.23.2 TRAVEL AUTHORIZATION REQUESTS

Before undertaking travel to any Government site or any other site in performance of this Contract, the contractor shall have this travel approved by, and coordinated with, the FEDSIM COR. Notification shall include, at a minimum, the number of persons in the party, traveler name, destination, duration of stay, purpose, and estimated cost. Prior to any long distance travel, the contractor shall prepare a Travel Authorization Request for Government review and approval. Long distance travel will be reimbursed for cost of travel comparable with the FTR, JTR, and DSSR, as applicable.

Requests for travel approval shall:

- Be prepared in a legible manner.
- Include a description of the travel proposed including a statement as to purpose.
- Be summarized by traveler.
- Identify the TO number.
- Identify the CLIN and Interagency Agreement account associated with the travel.
- Be submitted in advance of the travel with sufficient time to permit review and approval.

The contractor shall use only the minimum number of travelers and rental cars needed to accomplish the task(s). Travel shall be scheduled during normal duty hours whenever possible.

H.24 ODCs

The Government may require the contractor to purchase hardware, software, and related supplies critical and related to the services being acquired under the TO. Such requirements will be identified at the time a TOR is issued or may be identified during the course of a TO by the Government or the contractor. If the contractor initiates a purchase within the scope of this TO and the prime contractor has an approved purchasing system, the contractor shall submit to the

FEDSIM COR a Request to Initiate Purchase (RIP). If the prime contractor does not have an approved purchasing system, the contractor shall submit to the CO a Consent to Purchase (CTP). The RIP and CTP shall include the purpose, specific items, estimated cost, cost comparison, and rationale. The contractor shall not make any purchases without an approved RIP from the COR or an approved CTP from the CO.

H.25 TRANSFER OF HARDWARE/SOFTWARE MAINTENANCE AGREEMENTS

If the offeror proposes to provide any commercial computer software ("Commercial Software") as part of its proposed solution in response to this Solicitation, the offeror shall ensure that any software license agreement ("License Agreement") associated with such Commercial Software and intended to bind the Government complies with the FAR clause at 12.212(a), which provides, in relevant part, that commercial computer software and documentation shall be acquired under licenses customarily provided to the public "to the extent such licenses are consistent with Federal law." The most common examples of areas of non-compliance are set forth in the table below, which is provided for information purposes only and does not constitute an exhaustive list.

The requirement to propose compliant License Agreements shall apply regardless of whether the original rights holder to the Commercial Software ("Licensor") is the offeror, its subcontractor, or a third party, in the case of third-party software embedded or provided with the Commercial Software. Further, this requirement shall apply regardless of the format or title of the License Agreement (i.e., whether entitled "Software License Agreement," "End User License Agreement," "Terms of Service," or otherwise and whether presented in hard copy or in a clickwrap or other electronic format). For the avoidance of doubt, this may require the offeror to negotiate with its Licensors and to obtain a revised version of the License Agreement. License Agreements incorporated into a company's existing Schedule 70 or other Government contract are not exempt from this requirement.

If proposing Commercial Software, the offeror shall include a statement in its proposal certifying that all applicable License Agreements will comply with the requirement of Section H.25 (actual License Agreements need not be submitted prior to award). Failure to certify compliance will render the proposal ineligible for award, and non-compliance identified after award may entitle the Government to terminate the contract and seek any or all available remedies for breach of contract.

Commercial Terms*	Legal Restriction	Action**
Contract Formation and Modification	Under FAR 1.601(a), in an acquisition involving the use of appropriated funds, an agreement binding on the Government may only be entered into by a duly warranted CO in writing. Under FAR 43.102, the same requirement applies to contract modifications affecting the rights of the parties.	Any provisions purporting to form a contract binding on the U.S. Government by any other means (e.g., use, download, click through terms, etc.) must be deleted. The same applies to provisions allowing for License Agreement terms to be changed unilaterally by the Licensor.
Patent or Other Type of Intellectual Property Indemnity – sellers of products or services often provide that in the event of claim or litigation alleging infringement of patent rights asserted by some third party that the seller will indemnify the buyer, provided that the buyer provide notice of the claim or litigation, and that the seller assume control of the litigation and any proposed settlement.	Under the authority of 28 U.S.C. § 516, only the Attorney General, acting by and through the attorneys of the U.S. Department of Justice, may represent the U.S. Government in litigation.	The patent or other type of intellectual property indemnity clause remains in effect, but any undertaking to "defend" the Government or any requirement that the seller control litigation and/or any proposed settlement is to be deleted.
General Indemnity – sellers of products or services provide that in the event of any litigation arising from the buyers use of the product or service that buyer will indemnify seller's litigation costs and damages (if any).	Agreements to pay the attorney fees of a private party require a statutory waiver of sovereign immunity. Agreements to pay some indeterminate amount of money in the future violate the restrictions of the Anti-Deficiency Act, 31 U.S.C. § 1341(a)(1) and the Adequacy of Appropriations Act, 41 U.S.C. §11.	General Indemnity clauses must be removed from the License Agreement.

Commercial Terms*	Legal Restriction	Action**
Arbitration of Disputes – sellers of products or services provide that any disputes with buyer must be resolved through binding arbitration without recourse to litigation in state or federal courts.	Federal Agencies are not allowed to use binding arbitration unless the head of the agency has promulgated guidance through administrative rulemaking on the use of binding arbitration. *See* 5 U.S.C. § 575. At the time of this Solicitation release, GSA has not done so.	Binding Arbitration clauses must be removed from the License Agreement.
Venue, Jurisdiction and Choice of Law – sellers of products or services provide that jurisdiction of any dispute will be in a particular state, federal or foreign court or that particular state or foreign law will govern.	Litigation where the U.S. Government is a defendant must be heard either in U.S. District Court (28 U.S.C. § 1346) or the U.S. Court of Federal Claims (28 U.S.C. §1491). The U.S. Government, as the sovereign, does not contract under state or foreign law. Depending on the subject matter of the dispute, the Contract Disputes Act or other applicable law will govern.	Clauses claiming that disputes will only be heard in state court will be revised to allow disputes in Federal court. Choice of law clauses must be deleted.
Equitable Remedies – sellers of products or services provide that in the event of a dispute concerning patent or copyright infringement that the end user agree that an injunction is appropriate.	The only remedy provided for copyright or patent infringement against the U.S. Government is monetary damages. *See* 28 U.S.C. § 1498.	Equitable remedy clauses must be removed.
Negative Options – sellers of products or services provide that option periods will automatically be exercised unless affirmative action is taken by the buyer to not exercise the option.	Agreements to pay money in advance of appropriations violate the restrictions of the Anti-Deficiency Act, 31 U.S.C. § 1341(a)(1) and the Adequacy of Appropriations Act, 41 U.S.C. §11.	Negative option clauses must be removed.

Commercial Terms*	Legal Restriction	Action**
Limitation of Liability	Various (see next column)	Limitation of liability clauses may be included in accordance with the Licensor's standard commercial practices, except that such clauses may not operate to impair or prejudice the U.S. Government's right (a) to recover for fraud or crimes arising out of or relating to this TO under any Federal fraud statute, including without limitation the False Claims Act (31 U.S.C. §§3729 through 3733), or (b) to express remedies provided under any FAR, GSAR or master Alliant contract clauses incorporated into this TO.
Integration/Order of Precedence Clauses		Any provisions purporting to invalidate or supersede the terms of the Government TO resulting from this Solicitation (such provisions are frequently found in "entire agreement" clauses) must be removed from the License Agreement.

* The following standard commercial terms are deemed non-compliant within the meaning of this clause.
** The License Agreement will be deemed compliant when the action specified in this column is successfully implemented.

H.27 CONTRACTOR IDENTIFICATION

As stated in 48 CFR 211.106, Purchase Descriptions for Service Contracts, contractor personnel shall identify themselves as contractor personnel by introducing themselves or being introduced as contractor personnel and by displaying distinguishing badges or other visible identification for meetings with Government personnel. Contractor personnel shall appropriately identify themselves as contractor employees in telephone conversations and in formal and informal written correspondence.

H.28 INTELLECTUAL PROPERTY RIGHTS

The existence of any patent, patent application or other intellectual property right that encumbers any deliverable must be disclosed in writing on the cover letter that accompanies the delivery. If no such disclosures are provided, "the data rights provisions in FAR 52.227-14 apply.

NOTE: The section numbers in this TO correspond to the section numbers in the Alliant Contract. Section I of the contractor's Alliant Contract is applicable to this TO and is hereby incorporated by reference. In addition, the following applies:

I.2 FAR 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This TO incorporates one more clauses by reference with the same force and effect as if they were given in full text. Upon request the CO will make their full text available. The full text of a provision may be accessed electronically at:

FAR website: https://www.acquisition.gov/far/

Clause No	Clause Title	Date
52.204.10	Reporting Executive Compensation and First Tier Subcontract Awards	(Jul 2010)
52.215-21	Requirements for Cost or Pricing Data or Information Other than Cost or Pricing Data – Modifications	(Oct 2010)
52.216-8	Fixed Fee	(Jun 2011)
52.217-8	Option to Extend Services Fill-In Date: 30 days Prior to expiration of Task Order	(Nov 1999)
52.217-9	Option to Extend the Term of the Contract: 30 days prior to expiration of Task Order	(Mar 2000)
52.219-8	Utilization of Small Business Concerns	(Jan 2011)
52.219-9	Small Business Subcontracting Plan	(Jan 2011)
52.223-15	Energy Efficiency in Energy Consuming Products	(Dec 2007)
52.223-16	IEEE 1680 Standard for the Environmental Assessment of Personal Computer Products	(Dec 2007)
	Deleted	
	Deleted	
	Deleted	
52.232-18	Availability of Funds	(Apr 1984)
52.232-20	Limitation of Cost	(Apr 1984)
52.232-22	Limitation of Funds	(Apr 1984)
52.244-6	Subcontracts for Commercial Items	(Dec 2010)
52.251-1	Government Supply Sources	(Aug 2010)

I.3 GENERAL SERVICES ADMINISTRATION ACQUISITION MANUAL (GSAM), INCORPORATED BY REFERENCE

The full text of a provision may be accessed electronically at:

GSAM website: https://www.acquisition.gov/gsam/gsam.html

Clause No	Clause Title	Date

Clause No	Clause Title	Date
552.232.25	Prompt Payment	(Nov 2009)

NOTE: Insert appropriate Agency supplemental clauses, as required. Include the following for DoD clients, and update accordingly.

I.15 DEFENSE FEDERAL ACQUISITION REGULATION SUPPLEMENTS (DFARS) CLAUSES INCORPORATED BY REFERENCE

The full text of a provision may be accessed electronically at:

Defense Procurement website: www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html

Clause No	Clause Title	Date
252.204-7004	Alternate A, Central Contractor Registration	(Sep 2007)
252.227-7013	Rights in Technical Data - Noncommercial Items	(Mar 2011)
252.227-7014	Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation	(Mar 2011)
252.227-7016	Rights in Bid or Proposal Information	(Jan 2011)
252.227-7019	Validation of Asserted Restrictions - Computer Software	(Jun 1995)
252.227-7028	Technical Data or Computer Software Previously Delivered to the Government	(Jun 1995)
252.246-7001	Warranty of Data	(Dec 1991)

The information provided in Section J is for reference only. The documents in Section J are not intended to change the Task Order and any conflict therein should be resolved by referring and relying upon the Task Order. Because the Section J reference materials may be outdated or contain information that has not been recently verified for accuracy, the Government does not warrant the accuracy of the information for purposes of this Task Order.

J.1 LIST OF ATTACHMENTS

Attachment	Title
A	Monthly Status Report
B	Department of Defense (DD) 254 (separately attached .pdf)
C	Travel Authorization Template (electronically attached .xls)
D	Consent to Purchase Template (electronically attached .xls)
E	Request to Initiate Purchase Template (electronically attached .xls)
F	Employee/Contractor Non-Disclosure Agreement
G	Removed for Award
H	Problem Notification Report
I	Deliverable Acceptance-Rejection Report
J	Negotiated Ceiling Rates –Listed in Section B (not applicable)
K	Removed for Award
L	Removed for Award
M	Removed for Award
N	Draft Quality Assurance Surveillance Plan (QASP)

Attachment A
Monthly Status Report

ATTACHMENT A

MONTHLY STATUS REPORT FOR (MONTH AND YEAR)

Contractor Name
Task Order Number
Prepared by:
Reporting Period:
Page 1 of __

Monthly Status Report

Work Planned for the Month

Work Completed During the Month

Work Not Completed During the Month

Work Planned for Next Month

Contract Meetings
Indicate the meeting date, meeting subject, persons in attendance and duration of the meeting.

Deliverable Status

Issues/Questions/Recommendations

Risks
Indicate potential risks, their probability, impact, and proposed mitigation strategy.

Funds/Hours Expended
Total hours expended by the contractor during the week. Total funds expended by the contractor during the week.

Attachment B
Department of Defense (DD) 254 (Separately attached)

Attachment C
Travel Authorization Template (electronically attached .xls)

REQUEST FOR TRAVEL AUTHORIZATION

Contract Number: **Delivery Order No.:**
Project Title:
Travel Authorization No.
PMP / WBS / Number:
Name of Traveler:
Company:
CLIN Number:
Origination:
Destination:
Dates of Travel:
Organization(s) to be Visited:
Purpose of Travel:
Requested by:
Trip Report Required:

		Daily Amt	No of Days	Totals
Estimate of Approved	Airfare			0.00
Travel Funds including	Rental Car			0.00
G&A:	Lodging			0.00
	MIE			0.00
	Parking at Airport			0.00
	Other: POV & Gas, Phone			0.00
	Subtotal			0.00
	G&A			
	Total			**0.00**

Program Manager

Attachment D
Consent to Purchase Template (electronically attached .xls)

CONSENT TO PURCHASE TEMPLATE

Request #:
Date:
From: (IP)
TO: FEDSIM

Subject: Consent to Purchase
WBS: **X.X**

Reference: Contract Number XXXXXXXX/Task Order No. XXXXXXXX

(IP), in support of the (client) requests consent to purchase the below services under CLIN No. XXXX of the referenced contract. The cost of these items, when added to all other items purchased under CLIN XXXX does not exceed the funded amount of CLIN No. XXXX.

Justification for Purchase:

Qty	**Unit**	**Description**	**Unit Price**	**Total**
			Subtotal	
			Sales Tax	
			Shipping & Handling (approx.)	
			Other	
			Total	

Recommended Source:	**Justification for Source Selection:**
Additional Comments	***(client) Approving Officials:***
(client) Technical POC:	**Date:**
(client) POC:	
Ship To:	**Items Required On/Before:**

Attachment E
Request to Initiate Purchase Template (electronically attached .xls)

Attach E -Request to Initate Purchase Tem

Attachment F
Employee/Contractor Non-Disclosure Agreement

NON-DISCLOSURE AGREEMENT
BETWEEN
U.S. GENERAL SERVICES ADMINISTRATION (GSA)
FEDERAL SYSTEMS INTEGRATION AND MANAGEMENT CENTER (FEDSIM)
AND
[CONTRACTOR]

This agreement, made and entered into this _____ day of _____, 20XX (the "Effective Date"), is by and between GSA and [CONTRACTOR].

WHEREAS, [CONTRACTOR] and GSA FEDSIM have entered into [Contract No.], Task Order No. [INSERT] for services supporting the [CLIENT AGENCY AND PROGRAM/PROJECT NAME];

WHEREAS, [CONTRACTOR] is providing [DESCRIPTION, e.g., consulting/professional IT, engineering] services under the Task Order;

WHEREAS, the services required to support [PROGRAM/PROJECT NAME] involve certain information which the Government considers to be "Confidential Information"[1] as defined herein;

WHEREAS, GSA desires to have [CONTRACTOR]'s support to accomplish the Task Order services and, therefore, must grant access to the Confidential Information;

WHEREAS, [CONTRACTOR] through its work at a Government site may have access to Government systems or encounter information unrelated to performance of the Task Order which also is considered to be Confidential Information as defined herein;

WHEREAS, GS on behalf of [CLIENT AGENCY] desires to protect the confidentiality and use of such Confidential Information;

NOW, THEREFORE, for and in consideration of the mutual promises contained herein, the parties agree as follows:

1. **Definitions.** "Confidential Information" shall mean any of the following: (1) "contractor bid or proposal information" and "source selection information" as those terms are defined in 41 U.S.C. § 2101; (2) the trade secrets or proprietary information of other companies; (3) other information, whether owned or developed by the Government, that has not been previously made available to the public, such as the requirements, funding or budgeting data of the Government; and *for contracts/orders providing acquisition assistance,* this term specifically includes (4) past performance information, actual/proposed costs, overhead rates, profit, award fee determinations, contractor employee data of offerors/contractors, methods or procedures used to evaluate performance, assessments, ratings or deliberations developed in an evaluation process, the substance of any discussions or deliberations in an evaluation

[1] This does not denote an official security classification.

process, and any recommendations or decisions of the Government unless and until such decisions are publicly announced. This term is limited to unclassified information.

2. **Limitations on Disclosure.** [CONTRACTOR] agrees (and the [CONTRACTOR] Task Order personnel must agree by separate written agreement with CONTRACTOR) not to distribute, disclose or disseminate Confidential Information to anyone beyond the personnel identified in the [ATTACHED ADDENDUM], unless authorized in advance by the GSA Contracting Officer in writing. The Contracting Officer and [CLIENT POC] will review the Addendum to ensure it includes only those individuals to be allowed access to the information. The Addendum, which may be updated from time to time, is approved when signed by the GSA Contracting Officer and [CLIENT POC].

3. **Agreements with Employees and Subcontractors.** [CONTRACTOR] will require its employees and any subcontractors or subcontractor employees performing services for this Task Order to sign non-disclosure agreements obligating each employee/subcontractor employee to comply with the terms of this agreement. [CONTRACTOR] shall maintain copies of each agreement on file and furnish them to the Government upon request.

4. **Statutory Restrictions Relating to Procurement Information.** [CONTRACTOR] acknowledges that certain Confidential Information may be subject to restrictions in Section 27 of the Office of Federal Procurement Policy Act (41 U.S.C. § 2104), as amended, and disclosures may result in criminal, civil, and/or administrative penalties. In addition, [CONTRACTOR] acknowledges that 18 U.S.C. § 1905, a criminal statute, bars an employee of a private sector organization from divulging certain confidential business information unless authorized by law.

5. **Limitations on Use of Confidential Information.** [CONTRACTOR] may obtain Confidential Information through performance of the Task Order orally or in writing. These disclosures or this access to information is being made upon the basis of the confidential relationship between the parties and, unless specifically authorized in accordance with this agreement, [CONTRACTOR] will:
   a) Use such Confidential Information for the sole purpose of performing the [PROGRAM/PROJECT] support requirements detailed in the Task Order and for no other purpose;
   b) Not make any copies of Confidential Information, in whole or in part;
   c) Promptly notify GSA in writing of any unauthorized misappropriation, disclosure, or use by any person of the Confidential Information which may come to its attention and take all steps reasonably necessary to limit, stop or otherwise remedy such misappropriation, disclosure, or use caused or permitted by a [CONTRACTOR] employee.

6. **Duties Respecting Third Parties.** If [CONTRACTOR] will have access to the proprietary information of other companies in performing Task Order support services for the Government, [CONTRACTOR] shall enter into agreements with the other companies to protect their information from unauthorized use or disclosure for as long as it remains proprietary and refrain from using the information for any purpose other than that for which

it was furnished. [CONTRACTOR] agrees to maintain copies of these third party agreements and furnish them to the Government upon request in accordance with 48 C.F.R. § 9.505-4(b).

7. **Notice Concerning Organizational Conflicts of Interest.** [CONTRACTOR] agrees that distribution, disclosure or dissemination of Confidential Information (whether authorized or unauthorized) within its corporate organization or affiliates, may lead to disqualification from participation in future Government procurements under the organizational conflict of interest rules of 48 C.F.R. § 9.5.

8. **Entire Agreement.** This Agreement constitutes the entire agreement between the parties and supersedes any prior or contemporaneous oral or written representations with regard to protection of Confidential Information in performance of the subject Task Order. This Agreement may not be modified except in writing signed by both parties.

9. **Governing Law**. The laws of the United States shall govern this agreement.

10. **Severability.** If any provision of this Agreement is invalid or unenforceable under the applicable law, the remaining provisions shall remain in effect.

    In accordance with Public Law No. 108-447, Consolidated Act, 2005, the following is applicable:

    > These restrictions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by Executive Order No. 12958; section 7211 of title 5, United States Code (governing disclosures to Congress); section 1034 of title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); section 2302(b)(8) of title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that could expose confidential Government agents); and the statutes which protect against disclosure that may compromise the national security, including sections 641, 793, 794, 798, and 952 of title 18, United States Code, and section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. 783(b)). The definitions, requirements, obligations, rights, sanctions, and liabilities created by said Executive order and listed statutes are incorporated into this agreement and are controlling.

11. **Beneficiaries.** If information owned by an individual or entity not a party to this agreement is disclosed or misappropriated by [CONTRACTOR] in breach of this agreement, such information owner is a third party beneficiary of this agreement. However, nothing herein shall create an independent right of action against the U.S. Government by any third party.

IN WITNESS WHEREOF, GSA and [CONTRACTOR] have caused the Agreement to be executed as of the day and year first written above.

UNITED STATES GENERAL SERVICES ADMINISTRATION

_____ _____
Name Date

_____
Contracting Officer

[CONTRACTOR]

_____ _____
Name* Date

_____
Title

*Person must have the authority to bind the company.

Attachment G
Removed for Award

Attachment H
Problem Notification Report

PROBLEM NOTIFICATION REPORT

TASK ORDER NUMBER: _____ DATE: _____

1. Nature and sources of problem:

2. COTR was verbally notified on: (date) _____

3. Is action required by the Government? Yes_____ No_____

4. If YES, describe Government action required and date required:

5. Will problem impact delivery schedule? Yes_____ No_____

6. If YES, identify what deliverables will be affected and extent of delay:

7. Can required delivery be brought back on schedule? Yes_____ No_____

8. Describe corrective action needed to resolve problems:

9. When will corrective action be completed?

10. Are increased costs anticipated? Yes_____ No_____

11. Identify amount of increased costs anticipated, their nature, and define Government responsibility for problems and costs:

Attachment I
Deliverable Acceptance-Rejection Report

DELIVERABLE ACCEPTANCE/REJECTION FORM

Dear (insert name of COTR)

Please review the deliverable identified below, sign and date, and provide any comments either in the space provided or on an attached form. Comments are due by **XX/XX/20XX**.

DELIVERABLE NAME:
AGENCY NAME:
PROJECT NAME:
FEDSIM TASK ORDER/CONTRACT NUMBER:
FEDSIM PROJECT NUMBER:
DELIVERABLE DUE DATE:

I have reviewed the aforementioned document and have:
☐ Accepted it without comments
☐ Accepted it with comments
☐ Rejected it with comments

COMMENTS:

_____ _____
(name) (date)
(title)

Attachment J
Negotiated Ceiling Rates
Listed in Section B
Not Applicable

Attachment K
Removed for Award

Attachment L
Removed for Award

Attachment M
Removed for Award

Attachment N
Draft Quality Assurance Surveillance Plan (QASP)

DC3 QASP 10-25-11 1035.docx